Satisfiability thresholds beyond $k-$XORSAT

Andreas Goerdt, Lutz Falke

Technische Universität Chemnitz, Fakultät für Informatik
Straße der Nationen 62, 09107 Chemnitz, Germany
{goerdt, falu}@informatik.tu-chemnitz.de ,
http://www.tu-chemnitz.de/informatik/TI/

Abstract. We consider random systems of equations $x_1 + \cdots + x_k = a$, $0 \leq a \leq 2$ which are interpreted as equations modulo 3. We show for $k \geq 15$ that the satisfiability threshold of such systems occurs where the $2-$core has density 1. We show a similar result for random uniquely extendible constraints over 4 elements. Our results extend previous results of Dubois/Mandler for equations $\mod 2$ and $k = 3$ and Connamacher/Molloy for uniquely extendible constraints over a domain of 4 elements with $k = 3$ arguments.
Our proof technique is based on variance calculations, using a technique introduced Dubois/Mandler. However, several additional observations (of independent interest) are necessary.

1 Introcuction

1.1 Contribution

Often constraints are equations of the type $f(x_1, \ldots, x_k) = a$ where a is an element of the domain considered and f is a $k-$ary function on this domain, for example addition of k elements. Given a formula, which is a conjunction of m constraints over n variables we want to find a solution. It is natural to assume that f has the property: Given $k - 1$ arguments we can always set the last argument such, that the constraint becomes true. In this case we can restrict attention to the $2-$core. It is obtained by iteratively deleting all variables which occur at most once. Thus it is the maximal subformula in which each variable occurs at least twice.

We consider the random instance $F(n, p)$: Each equation over n variables is picked independently with probability p; the domain size d and the number of slots per equation k is fixed. We consider the case $p = c/n^{k-1}$ and the number of constraints is linear in n whp. (with high probability, that is probability $1 - o(1), n$ large.) The density of a formula is equal to the number of equations divided by the number of variables. The following is well known:

Fact 1 ([2]) *1. Conditional on the number of variables n' and equations m' of the $2-$core the $2-$core is a uniform random member of all formulas where each variable occurs at least twice.*

2. There exist $n' = n'(c)$ and $m' = m'(c)$ such that the number of variables of the $2-$core is $n'(1 + o(1))$ and the number of equations $m'(1 + o(1))$ whp.
3. There exists a T such that whp. for $c \leq T - \varepsilon$ the $2-$core has density $\leq 1 - \varepsilon$ and for $c \geq T + \varepsilon$ the $2-$core has density $\geq 1 + \varepsilon$. T is determined as the solution of an analytical equation.

The expected number of solutions of the $2-$core is d^{n-m}, n the number of variables, m the number of equations. When the $2-$core has density $\geq 1 + \varepsilon$ whp. no solution exists. This holds in particular when the density of $F(n, p)$ itself is $\geq 1 + \varepsilon$. The formulas considered here always have density < 1. In seminal work Dubois and Mandler [8] consider equations $\mod 2 : x_1 + \ldots + x_k = a, 0 \leq a \leq 1, k = 3$. They show satisfiability whp. when the 2-core has density $\leq 1 - \varepsilon$. For larger $k \geq 15$ a full proof for this result is given in [5], Appendix C . Thus T/n^{k-1} is the threshold for unsatisfiability in this case.

It is a natural conjecture that the same threshold applies to equations as discussed initially (and to some other types.) However, it seems difficult to prove the conjecture in some generality. One of the difficulties seems to be that we have 2 parameters k and d. We make some progress towards this conjecture. We show it for equations $\mod 3$. (The result is for $k > 15$, but we think it mainly technical to get it for all $k \geq 3$.)

Theorem 2 *Let $F(n, p)$ be the random set of equations $\mod 3 : x_1 + \cdots + x_k = a, 0 \leq a \leq 2, x_1 + \cdots + x_k$ an ordered $k - tuple$ of variables. If $p < (T - \varepsilon)/n^{k-1}$ $F(n, p)$ is satisfiable whp. for $k > 15$.*

The main task is to show that a $2-$core of density $\leq 1 - \varepsilon$ has a solution with probability $> \varepsilon > 0$. Our proof starts as Dubois/Mandler: Let X be the number of satisfying assignments of the $2-$core. Its expectation is $\geq d^{\varepsilon n}, d = 3$. We show that $E[X^2] \leq O(E[X])^2$. This implies (by Cauchy-Schwartz (or Paley-Zygmund) inequality) that the probability to have a solution is $\geq \varepsilon > 0$. By Fact 1 $F(n, p)$ has a solution with the same probability. We apply Friedgut-Bourgain's Theorem to $F(n, p)$ to show that unsatisfiability has a sharp threshold. By this the probability becomes $1 - o(1)$. In [9] Friedgut-Bourgain is applied to the $\mod 2-$case. It seems that our proof for the $\mod 3-$case is somewhat simpler (and applies to the $\mod 2-$case and other cases.)

To determine $E[X^2]$ Dubois/Mandler apply Laplace Method (one ingredient: bounding a sum through its maximum term.) The main difficulty is to bound a real function of several arguments from above. They show that their function has only one local maximum. We proceed by the same method, but substantial changes are necessary for $k > 3$.

First, we observe (cf. [5], Appendix C) that the function in question is $\leq$ the *infimum* with respect to certain other parameters. This is based on generating functions: If $f(x) = \sum c_k x^k$ then $c^k \leq f(a)/a^k$, $a > 0, c_i \geq 0$ (a method rarely used in the area, a notable exception is [16].) Thus to bound the maximum from above we need to find suitable parameters and show that the value with respect to these parameters is less than the required upper bound . (This leads to involved, but elementary calculus.)

To make this approach work we need appropriate generating functions: $X = X_{a_1} + \ldots X_{a_{3^n}}$, where X_{a_i} is the indicator random variable of the event that assignment a_i makes the formula true. Then $X^2 = \sum_a \sum_b X_a X_b$. To get $E[X^2]$ we need to determine Prob$[X_a X_b = 1]$. To this end we observe that the equation $x_1 + \cdots + x_k = c$ which is true under a is true exactly under those assignments b such that $0k_0 + 1k_1 + 2k_2 = 0 \mod 3$, and k_i is the number of slots of $x_1 + \cdots + x_k$ filled with a variable x with $b(x) = a(x) + i$. Thus there are $\sum_{k_1 = k_2 \mod 3} \binom{k}{k - k_1 - k_2, k_1, k_2}$ different ways in which an equation can become true under a, b. The following generating function allows us to deal with these possibilities analytically. With $\mathbf{w_1} = \exp(\mathbf{2}\pi\imath/\mathbf{3})$ the primitive third root of unity and $\mathbf{w_2} = \mathbf{w_1^2}$ we define $r(x_0, x_1, x_2) = \frac{1}{3}\left[(x_0 + x_1 + x_2)^k + (x_0 + \mathbf{w_1}x_1 + \mathbf{w_2}x_2)^k + (x_0 + \mathbf{w_2}x_1 + \mathbf{w_1}x_2)^k\right]$ then Coeff$[x_1^{k_1} x_2^{k_2}, r(1, x_1, x_2)] = \binom{k}{k - k_1 - k_2, k_1, k_2}$ if $k_1 = k_2 \mod 3$ and 0 otherwise (easy from properties $\mathbf{w_j}$.) In the $\mod 2-$case we use $1/2\left[(1 + x)^k + (1 - x)^k\right]$ instead [5], Appendix C.

With the motivation to get an exact threshold of unsatisfiability for a type of constraint whose worst-case complexity is NP-complete, Connamacher/Molloy [6] see also the very recent [17] introduce uniquely extendible constraints. A $k-$ary uniquely extendible constraint is a function from D^k to true, false with the property: Given values from D for any $k - 1$ argument slots there is exactly one value for the remaining slot which makes the constraint true. (The $k > 8$ in the following result can be eliminated at the price of some additional technical effort.)

Theorem 3 *Let $F(n, p)$ be the random formula of uniquely extendible constraints: Each constraint is a random $k-$tuple of variables and a $k-$ary uniquely extendible constraint over D and we pick with probability p. For $|D| = 4$ and $p < (T - \varepsilon)/n^{k-1}$ $F(n, p)$ is satisfiable whp. for $k > 8$.*

The threshold T/n^{k-1} is proved for $k = 3$ and $|D| = 4$, cf. [17] remark following Theorem 8. Our proof uses the technique as in the $\mod 3-$case, however the details are different. One of the contributions making is the generating polynomial
$p(x) = \frac{1}{d}\left[(1 + x)^k + (d - 1)(1 - \frac{x}{d-1})^k\right]$, as $r(x_0, x_1, x_2)$ above, not used before.

1.2 Motivation

Many computational problems can be naturally formulated as conjunctions of constraints. And we are interested to find a solution of this conjunction. Algorithmic properties of these conjunctions are considered in theoretical research (with remarkable results e. g. in the realm of approximation[3]) and applied research, e. g. [18]. An additional aspect is the investigation of conjunctions of randomly picked constraints; [7] is a fundamental study here. Propositional formulas in k-conjunctive normalform provide an example which has lead to a rich literature e. g. [1]. One of the characteristic properties of this research is that its findings can often be related to experimental work by running algorithms on randomly generated instances.

One of the aspects of random formulas is a threshold phenomenon: If the number of constraints of a conjunction picked is less than a threshold value the conjunction is typically satisfiable, if it is more we get unsatisfiability whp. Moreover instances picked close to the threshold seem to be algorithmically hard, thus being candidate test cases for algorithms. The threshold phenomenon and the possibility to investigate it by experiments causes physics to become interested in the area e. g. [11]. On the other hand, physical approaches lead to new algorithms and classical theoretical computer science research, e. g. [12].

One of the major topics is to determine the value of the threshold in natural cases. A full solution even in the natural $k-$CNF SAT case has not been obtained, but many partial results, [1] for $k = 3$. Note that $k-$CNF does not have the unique extendability property as possessed by the constraints considered here. And it seems to be a major open problem to get the precise threshold for constraints without unique extendibility and not similar to $2-$CNF. A mere existence result is the Friedgut-Bourgain theorem [13]. Based on this theorem thresholds for formulas of constraints over domains with more than 2 elements are considered in [7]. Ordering constraints are considered in [14], only partial results towards a threshold can be proven. In order to get definite threshold results further techniques are required. Therefore it is a useful effort to further develop the techniques with which thresholds can be proven. This is the general contribution of this paper.

A notable early exception, in that the precise threshold can be proven is the $\mod 2-$case considered above. Historically [8] is the first paper which uses variance calculation based on Laplace method in this area. Subsequently, for $k-$CNF SAT this method has lead to substantial progress in [15]. The contribution here is that $\mod 2-$proof can be refined and extended to cover other cases based on observations of independent interest. Note that random sparse linear systems over finite fields are used to construct error correcting codes, e. g. [19] or [20], motivating the $\mod 3-$case. A very recent study of the $\mod 2-$ case is [21]. More literature can be found in [10], but precise threshold results have not been obtained.

1.3 Contents

I. Equations modulo 3

1 Notation and basics

We use the abbreviation

$$M(m, n) := \sum_{v_1, \ldots v_n \geq 2} \binom{m}{v_1, \ldots v_n} \text{ and } N_0 := M(km, n). \text{ Then } N_0 \cdot 3^m \tag{1}$$

is the number of all formulas with k variables per equation and m equations. We consider the uniform distribution on the set of formulas. Note that the formulas we consider are $2-$cores. (Here the same equation to occur several times. This happens with probability $o(1)$ as m is linear in n and can be ignored.) Let X be the number of solutions of a formula. We have $X = \sum_a X_a$ where a stands for an assignment of the variables with $0, 1, 2$ and $X_a(F) = 1$ if F is true under a and 0 otherwise. The expectation of X is 3^{n-m} because given an assignment each equation is true independently with probability $1/3$. We assume that $m = \gamma n, \gamma$ bounded above by a constant < 1. As k is also constant, the asymptotics is only with respect to n. We need to show the following theorem

Theorem 4 $E[X^2] \leq C \cdot 3^{2(n-m)}$

We have $\mathrm{E}[X^2] = \sum_{(a,b)} \mathrm{E}[X_a \cdot X_b]$ where (a, b) refers to all ordered pairs of assignments.

Let $\overline{W} = (W_0, W_1, W_2)$ be a partition of the set of variables into 3 sets.We always use the notation $w_i = \sharp W_i,\ \bar{w} = (w_0, w_1, w_2)$. For two assignments we write $b = D(a, \overline{W})$ iff $W_i = \{x \,|\, b(x) = a(x) + i \mod 3\}$. We have that $a(x_1 + \cdots + x_k) = b(x_1 + \cdots + x_k)$ (Here $a(x_1 + \cdots + x_k)$ is the value of $x_1 + \cdots + x_k$ under a (analogously for b).) iff $\sum_{i=0,1,2} i \cdot \sharp\{j \,|\, x_j \in W_i\} = 0 \mod 3$. This is equivalent to $\sharp\{j \,|\, x_j \in W_1\} = \sharp\{j \,|\, x_j \in W_2\} \mod 3$. Given $\bar{l} = (l_0, l_1, l_2)$ with $\sum l_i = km$ we let $\mathcal{K}(\bar{l})$ be the set of all $3 \times m-$matrices $(k_{i,j})_{0 \leq i \leq 2, 1 \leq j \leq m}$ with $k_{1,j} = k_{2,j} \mod 3$ and each column sums to k, that is $\sum_i k_{i,j} = k$ for each j. Moreover, $\sum_j k_{i,j} = l_i$ for $i = 0, 1, 2$ (the i'th row sums to l_i.)

We denote

$$K(\bar{l}) := \sum_{(k_{i,j}) \in \mathcal{K}(\bar{l})} \prod_{j=1}^{m} \binom{k}{k_{0,j}\ ,\, k_{1,j}\ ,\, k_{2,j}}. \text{ Then } \hat{N}(\bar{w}, \bar{l}) := K(\bar{l}) \cdot \prod_{i=0}^{2} M(l_i, w_i) \quad (2)$$

is the number of formulas F true under two assignments a, b with $b = D(a, \overline{W})$ (with $w_i = \sharp W_i$) and the variables from W_i occupy exactly l_i slots of F. The factor $K(\bar{l})$ of $\hat{N}(\bar{w}, \bar{l})$ counts how the l_i slots available for W_i are distributed over the left-hand-sides of the equations. The second factor counts how to place the variables into their slots. Note that the right-hand-side of an equation cannot be chosen, it is determined by the value of the left-hand-side under a, b.

We abbreviate $\binom{n}{\bar{w}} = \binom{n}{w_0, w_1, w_2}$. Given an assignment a, $\bar{w}$, and $\bar{l}$, the number of assignment formula pairs (b, F) with : There exist $\overline{W}$ with $\sharp W_i = w_i$, such that $b \in D(a, \overline{W})$, F is true under a and b, and the variables from W_i occupy exactly l_i slots of F is

$$N(\bar{w}, \bar{l}) := \binom{n}{\bar{w}} \cdot \hat{N}(\bar{w}, \bar{l}). \text{ This implies } \mathrm{E}[X^2] = 3^n \cdot \sum_{\bar{w}, \bar{l}} N(\bar{w}, \bar{l}) \cdot \frac{1}{3^m \cdot N_0}. \quad (3)$$

Theorem 4 follows directly from the next theorem:

Theorem 5 $\sum_{\bar{w}, \bar{l}} N(\bar{w}, \bar{l}) / N_0 \leq C \cdot 3^{(1-\gamma)n}$.

One more piece of notation: $\omega_i = w_i / n$ usually is the fraction of variables belonging to W_i. And $\lambda_i = l_i / (km) = l_i / (k\gamma n)$ is the fraction of slots filled with a variable from W_i. We use $\bar{\omega} = (\omega_0, \omega_1, \omega_2)$, and $\bar{\lambda} = (\lambda_0, \lambda_1, \lambda_2)$. Sometimes ω_i, λ_i stand for arbitrary reals, this should be clear form the context.

2 Outline of the proof of Theorem 5

First, bounds for $M(m,n)$ and $K(\bar{l})$. We consider $q(x) := \exp(x) - x - 1 = \sum_{j\geq 2} \frac{x^j}{j!}$ for $x \geq 0$. Then for $a > 0$ and all m, n

$$M(m,n) \;=\; \text{Coeff}[x^m, q(x)^n] \cdot m! \;<\; q(a)^n \cdot \frac{1}{a^m} \cdot m! \;\leq\; q(a)^n \left(\frac{m}{a \cdot e}\right)^m \cdot O(\sqrt{m}) \quad (4)$$

using Stirling in the form $m! < (m/e)^m \cdot O(\sqrt{m})$.

To get rid of the $\sqrt{m}-$factor we let $Q(x) := xq'(x)/q(x)$ with $q'(x)$ the derivative of $q(x)$, $q'(x) = \exp(x) - 1$ for $x > 0$. Then $Q'(x) > 0$ for $x > 0$, $Q(x) > x$, and $Q(x) \longrightarrow 2$ for $x \longrightarrow 0$. Thus, for $y > 2$ the inverse function $Q^{-1}(y) > 0$ is defined and differentiable. Lemma 6 is proved in Section 5.

Lemma 6 *Let $Cn \geq m \geq (2+\varepsilon)n,\ C, \varepsilon > 0$ constants. Then*

$$M(m,n) \;=\; \Theta(1) \cdot \left(\frac{m}{ae}\right)^m \cdot q(a)^n \text{ with } a \text{ defined by } Q(a) = \frac{m}{n}$$

Throughout we use $s = s(k,\gamma)$ uniquely defined by $Q(s) = k\gamma = k\gamma n/n = km/n$. Note that for $k \geq 3$ we can assume that $k\gamma > 2$ and s always exists. We have $Q(s) \geq s$. We often write Q instead of $Q(s)$. Recall $N_0 = M(km,n)$ and we get a tight bound on the number of formulas (cf. (1).)

Corollary 7 $N_0 \;=\; \Theta(1)\, (k\gamma n/(se))^{k\gamma n} \cdot q(s)^n$.

We treat the sum $K(\bar{l})$ similarly to $M(m,n)$. Instead of $q(x)$ we use the function,

$$r(\bar{x}) := \sum_{k_1 = k_2 \mod 3} \binom{k}{k_0, k_1, k_2} x_0^{k_0} x_1^{k_1} x_2^{k_2},\ \ \bar{x} = (x_0, x_1, x_2).\ \text{Then}$$

$$K(\bar{l}) \;=\; \sum_{(k_{i,j}) \in \mathcal{K}(\bar{l})} \prod_{j=1}^{m} \binom{k}{k_{0,j}\,, k_{1,j}\,, k_{2,j}} \;=\; \text{Coeff}[\bar{x}^{\bar{l}},\, r(\bar{x})^m\,] \;<\; \frac{r(\bar{c})^m}{\bar{c}^{\bar{l}}} \quad (5)$$

with the notation $\bar{x}^{\bar{l}} = \prod_i x_i^{l_i}$ and $\bar{c} = (c_0, c_1, c_2) > 0$, meaning $c_i > 0$ for all i.

For calculations it is useful to have a different representation of $r(\bar{x})$. Let $\imath$ be the imaginary unit, and $\mathbf{w_1} := -1/2 + (\sqrt{3}/2)\imath$ is the primitive third root of unity, $\mathbf{w_2} := -1/2 - (\sqrt{3}/2)\imath \;=\; \mathbf{w_1}^2$. We have

$$r(\bar{x}) = \frac{1}{3}\left[(x_0 \,+\, x_1 \,+\, x_2)^k \,+\, (x_0 \,+\, \mathbf{w_1}x_1 + \mathbf{w_2}x_2)^k \,+\, (x_0 \,+\, \mathbf{w_2}x_1 \,+\, \mathbf{w_1}x_2)^k\right] (6)$$

The preceding equation is well known and easy to prove from basic properties of roots of unity. Note that in derivatives $\frac{d}{dx_i} r(\bar{x})$ the roots of unity are treated as constants.

For $x_i, y_i > 0$ we define (convention $\alpha^\alpha = 1$ for $\alpha = \omega_i$ or $\alpha = \lambda_i$ and $\alpha = 0$)

$$\Psi(\bar\omega\,,\,\bar\lambda\,,\,\bar x\,,\,\bar y\,) \;=\; \prod_{i=0,1,2}\left(\frac{q(x_i)}{\omega_i q(s)}\right)^{\omega_i}\cdot\left[\prod_{i=0,1,2}\left(\frac{\lambda_i s}{x_i y_i}\right)^{\lambda_i}\right]^{k\gamma} r(y_0,y_1,y_2)^{\gamma}$$

With $\omega_i = \lambda_i = 1/3, a_i = s(k,\gamma) = s$, and $c_i = 1$, we have $\Psi(\overline{\omega},\overline{\lambda},\bar a,\bar c) = 3\cdot(1/3)^{k\gamma}\cdot((1/3)3^k)^{\gamma} = 3^{1-\gamma}$ (use (6).)

Lemma 8 *$N(\bar w,\bar l)/N_0 \;<\; \Psi(\bar\omega\,,\,\bar\lambda\,,\,\bar a\,,\,\bar c\,)^n\cdot O(n)^{3/2}$ for any $\bar a,\bar c,a_i,c_i > 0$.*

Proof. $\binom{n}{\bar w} \le \prod_i (1/\omega_i)^{\omega_i n}$ for all $\bar w$, ([24], page 228) $\prod_{i=0,1,2} M(l_i,w_i)/N_0 \le \prod_i \left((l_i/(a_i e))^{l_i} q(a_i)^{w_i} O(\sqrt{l_i})\right)\cdot(es/(k\gamma n))^{k\gamma n}\cdot 1/q(s)^n\cdot O(1)$ with (4) and Corollary 7. Observe that $l_i = \lambda_i k\gamma n, \sum_i \lambda_i = 1, \sum\omega_i = 1$. Concerning $K(\bar l)$ apply (5).

For reals a,b we let $\mathcal{U}_\varepsilon(a,b) = \{(c,d)|\,|c-a|,|d-b| < \varepsilon\}$ be the open square neighborhood of (a,b). The notation $\bar\lambda,\bar\omega \in \mathcal{U}_\varepsilon(a,b)$ is used to mean $(\lambda_1,\lambda_2),(\omega_1,\omega_2) \in \mathcal{U}_\varepsilon(a,b)$. Theorem 9 is proved in Section 3.

Theorem 9 *For any $\bar\lambda > 0$ there exist $\bar a,\bar c > 0$ such that:*
(1) $\Psi(\bar\omega\,,\,\bar\lambda\,,\,\bar a\,,\,\bar c\,) \le 3^{1-\gamma}$.
(2) For any $\varepsilon > 0$, if $\bar\lambda \notin \mathcal{U}_\varepsilon(1/3,1/3)$ then $\Psi(\bar\omega\,,\bar\lambda\,,\bar a\,,\bar c) \le 3^{1-\gamma} - \delta$ for a $\delta > 0$.

Corollary 10 *Let $U = \mathcal{U}_\varepsilon(1/3,1/3)$ then $\sum_{\bar\lambda\notin U,\lambda_i>0,\bar\omega} N(\bar w,\bar l)/N_0 \;<\; C\cdot 3^{(1-\gamma)n}$.*

Proof. The sum has only $O(n^4)$ terms. With Lemma 8 and Theorem 9 (2) we see that each term is bounded above by $(3^{1-\gamma}-\delta)^n O(n)^{3/2}$.

To treat (λ_1,λ_2) close to $(1/3,1/3)$ we need a lemma analogous to Lemma 6 for $K(\bar l)$. Let the function $R(x_1,x_2) = (R_1(x_1,x_2),\,R_2(x_1,x_2))$ be defined by $R_i(x_1,x_2) = = x_i r_{x_i}(1,x_1,x_2)/r(1,x_1,x_2)$ for $i = 1,2$, $r_{x_i}(1,x_1,x_2)$ is the partial derivative of $r(1,x_1,x_2)$ wrt. x_i. The Jacobi Determinant of $R(x_1,x_2)$ is > 0 at $x_1 = x_2 = 1$ (proof Subsection 5.1.) Thus there is a neighborhood of $(1,1)$ in which $R(x_1,x_2)$ is invertible and the inverse function is differentiable. We have that $R(1,1) = (k/3,k/3)$. Thus for a suitable ε and $(\lambda_1,\lambda_2) \in \mathcal{U}_\varepsilon(1/3,1/3)$ we can define (c_1,c_2) by $R(c_1,c_2) = (k\lambda_1,k\lambda_2)$. Moreover, $c_i = c_i(\lambda_1,\lambda_2)$ is differentiable. Lemma 11 is proved in Subsection 5.1.

Lemma 11 *There is an $\varepsilon > 0$ such that for $(\lambda_1,\lambda_2) \in \mathcal{U}_\varepsilon(1/3,1/3)$*

$$K(\bar l) \;=\; O\left(\frac{1}{n}\right)\cdot\frac{r(1,c_1,c_2)}{c_1^{l_1}c_2^{l_2}} \text{ with } R(c_1,c_2) = (k\lambda_1,k\lambda_2) \text{ defining } c_1,c_2.$$

Corollary 12 *There is $\varepsilon > 0$ such that for $(\omega_1, \omega_2), (\lambda_1, \lambda_2) \in \mathcal{U}_\varepsilon(1/3, 1/3)$*

$$\frac{N(\bar{w}, \bar{l})}{N_0} \; \leq \; O\left(\frac{1}{n^2}\right) \Psi(\bar{\omega}\,,\; \bar{\lambda}\,,\; \bar{a}\,,\; \bar{c}\,)^n$$

where $Q(a_i) = l_i/w_i = \lambda_i k\gamma/\omega_i$ and $c_0 = 1$ and $R(c_1, c_2) = (\lambda_1 k, \lambda_2 k)$.

Comment. Observe that $\lambda_i k\gamma/\omega_i \;\approx\; k\gamma$, $a_i \approx s, c_i \approx 1$.

Proof. Our restriction on $\bar{\omega}$ implies that $\binom{n}{\bar{w}} \leq O(1/n) \prod_i (1/\omega_i)^{\omega_i n}$ (Stirling), giving us one $O(1/n)$. We get $\prod_i M(l_i, w_i)/N_0 \leq$ $\prod_i \left((l_i/(a_i e))^{l_i} q(a_i)^{w_i}\right) \cdot (es/(k\gamma n))^{k\gamma n} \cdot 1/q(s)^n \cdot O(1)$ applying Corollary 7 and Lemma 6 for the $M(l_i, w_i)$. Concerning $K(\bar{l})$ apply Lemma 11 which gives us a second factor $O(1/n)$. Otherwise the proof is as the proof of Lemma 8.

Lemma 13 is proved in Section 4.

Lemma 13 *The function $\Psi(\bar{\omega}\,,\; \bar{\lambda}\,,\; \bar{a}\,,\; \bar{c}\,)$ with a_i, c_i given by $Q(a_i) = \lambda_i k\gamma/\omega_i$ and $c_0 = 1$ and $R(c_1, c_2) = (\lambda_1 k, \lambda_2 k)$ has a local maximum with value $3^{1-\gamma}$ for $\lambda_i = \omega_i = 1/3$. In this case we get $a_i = s$ and $c_i = 1$.*

Corollary 14 *Let $U = \mathcal{U}_\varepsilon(1/3, 1/3)$, ε small enough. Then $\sum_{\bar{\omega} \notin U, \bar{\lambda} \in U, \lambda_i > 0} N(\bar{w}, \bar{l})/N_0 < C \cdot 3^{(1-\gamma)n}$.*

Proof. Let $\varepsilon > 0$ be such that $\Psi(\bar{\omega}, \bar{\lambda}, \bar{a}, \bar{c}) \leq 3^{1-\gamma}$ for $\bar{a}, \bar{c}$ as specified in Lemma 13 and $\bar{\omega}, \bar{\lambda} \in U$. Let $\bar{\omega} \notin U, \bar{\lambda} \in U$. We show $\Psi(\bar{\omega}, \bar{\lambda}, \bar{a}, \bar{c}) \leq 3^{1-\gamma} - \delta$ for some $\bar{a}, \bar{c}$. This implies the claim as in the proof of Corollary 10.

Let $\varepsilon' < \varepsilon/3$ and $U' = \mathcal{U}_{\varepsilon'}(1/3, 1/3)$. For $\bar{\lambda} \notin U'$ the claim follows with Theorem 9 (2). For $\bar{\lambda} \in U'$ we show that $\Psi(\bar{\omega}, \bar{\lambda}, \bar{a}, \bar{c}) \leq 3^{1-\gamma} - \delta$ for $a_i = s$ and $c_0 = 1, R(c_1, c_2) = (k\lambda_1, k\lambda_2)$. (Recall $\bar{\lambda} \in U$.) For $\Psi := \Psi(\bar{\lambda}, \bar{\lambda}, \bar{a}, \bar{c})$ with $\bar{a}, \bar{c}$ as required by Lemma 13 we have $\Psi \leq 3^{1-\gamma}$. Note, $Q(a_i) = \lambda_i k\gamma/\lambda_i = k\gamma$ which implies $a_i = s$ and $c_0 = 1, R(c_1, c_2) = (k\lambda_1, k\lambda_2)$. Therefore all a_i-terms cancel and $\Psi = \prod (1/\lambda_i)^{\lambda_i} \cdot \left(\prod (\lambda_i/c_i)^{\lambda_i k\gamma}\right) p(\bar{c})^\gamma \leq 3^{1-\gamma}$.

As $\bar{\omega} \notin U$ whereas $\bar{\lambda} \in U'$ and $\varepsilon' \leq \varepsilon/3$ we have that $\prod (1/\omega_i)^{\omega_i} \leq \prod (1/\lambda_i)^{\lambda_i} - \delta'$ for a $\delta' > 0$ (proof omitted.) Then $\Psi(\bar{\omega}, \bar{\lambda}, \bar{a}, \bar{c}) \leq \Psi - \delta' \left(\prod (\lambda_i/c_i)^{\lambda_i k\gamma}\right) p(\bar{c})^\gamma$. If $\Psi \leq 3/2$, we are done. Otherwise we have that $\left(\prod_i (\lambda_i/c_i)^{\lambda_i k\gamma}\right) p(\bar{c})^\gamma$ is bounded below by $1/2$ (as $\prod (1/\lambda_i)^{\lambda_i} \leq 3$) and the claim follows, with with $\delta = (1/2)\delta'$.

Theorem 15 is proved in Section 4 by Laplace method.

Theorem 15 *Let $U = \mathcal{U}_\varepsilon(1/3, 1/3)$. There is an $\varepsilon > 0$ such that*

$$\textstyle\sum_{\bar{\lambda}, \bar{\omega} \in U} N(\bar{w}, \bar{l})/N_0 \; < \; C \cdot 3^{(1-\gamma)n}.$$

Proof of Theorem 5. Pick ε such that Theorem 15 applies. Use Corollary 10, Corollary 14, and Theorem 15 and the sum of all terms $N(\bar{w}, \bar{l})/N_0$ with $l_i > 0$ is $\leq C \cdot 3^{(1-\gamma)n}$. Terms with an $l_i = 0$ do not add substantially to the sum (proof omitttted.) □

3 Proof of Theorem 9

We use the notation $\bar{x} = (x_0, x_1, x_2), \bar{y} = (y_0, y_1, y_2)$ and define

$$\begin{aligned}
\mathrm{OPT}_1(\bar{x}, s) \;&=\; \frac{q(sx_0)}{q(s)} + \frac{q(sx_1)}{q(s)} + \frac{q(sx_2)}{q(s)} \\
\mathrm{OPT}_2(\bar{x}, \bar{y}, s) \;&=\; \left(\frac{1}{x_0y_0 + x_1y_1 + x_2y_2}\right)^Q, \; x_0y_0 + x_1y_1 + x_2y_2 > 0 \\
\mathrm{OPT}_3(\bar{y}, s) \;&=\; (y_0 + y_1 + y_2)^Q \;+\; 2 \cdot \left(y_0^2 \;+\; y_1^2 \;+\; y_2^2 \;-\; y_0y_1 \;-\; y_0y_2 \;-\; y_1y_2\right)^{1/2 \cdot Q} \\
\mathrm{OPT}(\bar{x}, \bar{y}, s) \;&=\; \mathrm{OPT}_1(\bar{x}, s) \cdot \mathrm{OPT}_2(\bar{x}, \bar{y}, s) \cdot \mathrm{OPT}_3(\bar{y}, s).
\end{aligned}$$

Observe that $\mathrm{OPT}(1,1,1,1,1,1,s) = 3(1/3)^Q 3^Q = 3 = \mathrm{OPT}_1(1,1,1,s)$, $\mathrm{OPT}(1,0,0,1,0,0,s) = 1 \cdot (1/1)^Q \cdot 3 = 3 = \mathrm{OPT}_3(1,0,0,s)$. The following lemma shows the idea of OPT.

Lemma 16 *Given $\bar{\lambda} > 0$ and let λ be the maximum of the λ_i. Let $a_i, c_i > 0$ be such that $P_i := a_ic_i = \lambda_i/\lambda$. Then*

$$\Psi := \Psi(\bar{\omega}, \bar{\lambda}, \bar{a} \cdot s, \bar{c}) \leq \frac{1}{3^\gamma} \mathit{OPT}(\bar{a}, \bar{c}, s).$$

Proof. The factors of Ψ one by one: The first factor: The AGM-inequality gives $\prod_{i=0,1,2} \left(\frac{q(a_is)}{\omega_i q(s)}\right)^{\omega_i} \leq \mathrm{OPT}_1(\bar{a}, s)$. (Applies for $\omega_i = 0$, too.)

The second factor: We have $P_0 + P_1 + P_2 = a_0c_0 + a_1c_1 + a_2c_2 = 1/\lambda$ and $\lambda_i / a_ic_i = \lambda$ for $i = 0, 1, 2$. Recall $Q = k\gamma$, and the second factor of Ψ =

$$\prod_{i=0,1,2} \left(\frac{\lambda_i s}{a_isc_i}\right)^{\lambda_i k\gamma} = \lambda^{k\gamma} = \left(\frac{1}{a_0c_0 + a_1c_1 + a_2c_2}\right)^Q = \mathrm{OPT}_2(\bar{a}, \bar{c}, s).$$

The third factor: We let $C_1 = \sum_i c_i$ and $C_2 = \sum_i c_i^2 - c_0c_1 - c_0c_2 - c_1c_2$. Then $r(\bar{c}) = |r(\bar{c})| \leq (1/3)(C_1^k + 2C_2^{k/2})$ by the triangle inequality and as $|c_0 + \mathbf{w_1}c_1 + \mathbf{w_2}c_2| = [(c_0 - 1/2 \cdot (c_1 + c_2))^2 + (\sqrt{3}/2(c_1 - c_2))^2]^{1/2} = C_2^{1/2}$. Then $|r(\bar{c})|^\gamma \leq 1/3^\gamma (C_1^k + 2C_2^{k/2})^\gamma \leq 1/3^\gamma (C_1^{k\gamma} + 2^\gamma C_2^{\gamma k/2}) \leq 1/3^\gamma \mathrm{OPT}_3(\bar{c}, s)$ as $Q = k\gamma$, and as x^γ is concave (by $\gamma < 1$) we have $(y+z)^\gamma \leq y^\gamma + z^\gamma$.

The following picture shows $\mathrm{OPT}(1, a, a, 1, c, c, s),\ 0 \le a, c \le 1$. The $\le 3-$area is dark. We have a path from $a = c = 0$ to $a = c = 1$ through this area. Therefore, for all P with $0 \le P \le 1$ we have $0 \le a, c \le 1$ with $P = ac$ such that $\mathrm{OPT}(1, a, a, 1, c, c, s) \le 3$. In the notation of Lemma 16 this corresponds to $\lambda_0 \ge \lambda_1 = \lambda_2$ (and visualizes Theorem 9 for this case.) The following four lemmas are the technical core of our proof.

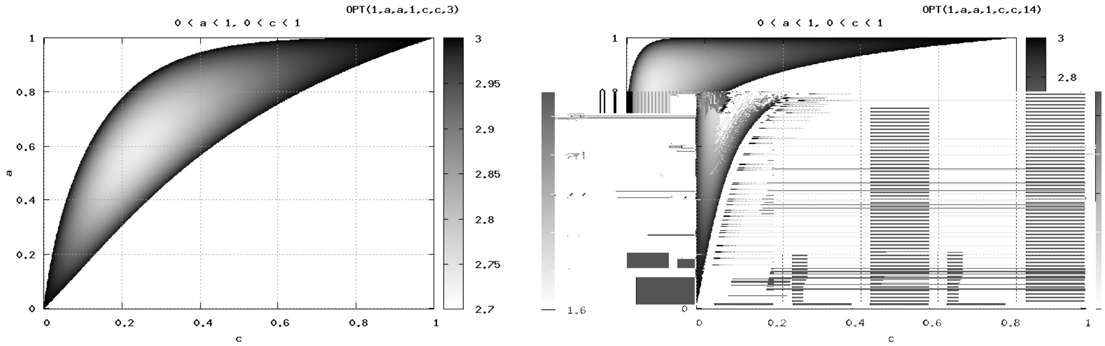


Fig. 1. $\mathrm{OPT}(1, a, a, 1, c, c, s)$ over the rectangle $0 \le a \le 1, 0 \le c \le 1$ for $s = 3$ and $s = 14$.

Lemma 17 *Let* $s \ge 8, A(x) = A(x, s) := (7/10)Q \cdot x$.
(a) OPT(y) $:=$ *OPT* $(1, A(y), A(y), 1, y, y, s)$ *is strictly decreasing for* $0 \le y \le 1/(2Q)$. *The start value is OPT*$(0) = 3$.
(b) Given $0 \le y \le 1/(2Q)$, *OPT*(z) $:=$ *OPT*$(1, A(y+z), A(y-z), 1, y+z, y-z, s)$ *is decreasing in* $0 \le z \le y$.

Lemma 18 *Let* $s \ge 7$ *, and* $\frac{7}{20} \le A \le 1 - \frac{1}{Q}$. *Then*
OPT(z) $:=$ *OPT*$(1, A, A, 1, 1/(2Q) + z, 1/(2Q) - z, s) \le 3 - \delta$ *for* $0 \le z \le 1/(2Q)$.

Lemma 19 *Let* $s \ge 7$, *and* $1/(2Q) \le C \le 1/2$. *Then*
OPT(z) $:=$ *OPT*$(1, 1 - 1/Q, 1 - 1/Q, 1, C + z, C - z, s) \le 3 - \delta$ *for* $0 \le z \le C$.

Lemma 20 *Let* $s \ge 15$ *and* $A(x) = A(x, s) := 1 + 7/(10Q) \cdot x - 7/(10Q)$.
(a) OPT(y) $:=$*OPT*$(1, A(y), A(y), 1, y, y, s)$ *is strictly increasing in* $4/10 \le y \le 1$. *The final value is OPT*$(1) = 3$.
(b) Given $4/10 \le y \le 1$, *OPT*(z) $:=$*OPT*$(1, A(y+z), A(y-z), 1, y+z, y-z, s)$ *is decreasing in* $0 \le z \le \min\{y, 1-y\}$.

Proof of Theorem 9 from the preceding lemmas. We prove Theorem 9 for $\lambda_0 \geq \lambda_1 \geq \lambda_2 > 0$ first. We denote $P_i := \lambda_i/\lambda_0,$ then $1 \geq P_1 \geq P_2 > 0$.
Case 1: $P_1 + P_2 \leq \frac{7}{20Q}$. With $A(x)$ from Lemma 17 we have $A(x) \cdot x = (7/10)Q \cdot x^2$. Thus there exist $y_1 \geq y_2$ with $P_i = A(y_i) \cdot y_i$. We represent y_i such that Lemma 17 is applicable.

$$y := \frac{y_1 + y_2}{2}, \; z := \frac{y_1 - y_2}{2}. \text{ Then } y_1 = y + z, y_2 = y - z, 0 \leq z \leq y.$$

We show $y \leq \frac{1}{2Q}$ and Lemma 17 applies to y, z.

$$\frac{7}{20Q} \geq P_1 + P_2 = \frac{7}{10}Q(y_1^2 + y_2^2) \Longrightarrow y_1^2 + y_2^2 \leq \frac{1}{2Q^2}.$$
$$(y_1 + y_2)^2 \leq 2y_1^2 + 2y_2^2 \leq \frac{1}{Q^2} \text{ and } y = \frac{y_1 + y_2}{2} \leq \frac{1}{2Q}.$$

With $a_0 = c_0 = 1, a_1 = A(y + z), a_2 = A(y - z), c_1 = y + z, c_2 = y - z$ we have $a_i c_i = P_i$. By Lemma 16 $\Psi := \Psi(\bar{\omega}, \bar{\lambda}, \bar{a} \cdot s, \bar{c}) \leq 1/3^{\gamma}\text{OPT}, \text{ OPT} := \text{OPT}(\bar{a}, \bar{c}, s)$. If $P_1 \geq \varepsilon$ for an $\varepsilon > 0$ we have OPT$< 3 - \delta'$ by Lemma 17 and Theorem 9 holds.

For smaller P_1 we have OPT ≤ 3, approaching 3. Only (1) of Theorem 9 holds. To get (2) for small P_1 we argue as follows: For P_1 approaching 0 we see that c_1 and c_2 approach 0. We consider the treatment of the factor $r(\bar{c})$ in the proof Lemma 16. Both C_1 and C_2 from this proof approach 1 in this case. Therefore we have a $\delta' > 0$ such that $(C_1^k + 2C_2^{k/2})^{\gamma} \leq C_1^{k\gamma} + 2^{\gamma}C_2^{k\gamma/2} - \delta'$. As $a_0 = c_0 = 1$ the first two factors of OPT do not approach 0. And we have $\Psi(\bar{\omega}, \bar{\lambda}, \bar{a} \cdot s, \bar{c}) \leq (1/3^{\gamma})(\text{OPT} - \delta'') \leq 3^{1-\gamma} - \delta$ and Theorem 9 (2) holds.
Case 2: $\frac{7}{20Q} \leq P_1 + P_2 \leq \left(1 - \frac{1}{Q}\right) \frac{1}{Q}$. To use Lemma 18 we define A by $A \cdot \frac{1}{Q} = P_1 + P_2$. and A is as required by Lemma 18. We need to find an appropriate z. As $P_1 \geq P_2$ there is a $y \geq \frac{1}{2}$ such that $P_1 = A\frac{1}{Q}y$ and $P_2 = A\frac{1}{Q}(1-y)$. With $y = \frac{1}{2} + z'$ and $1 - y = \frac{1}{2} - z', z' \leq \frac{1}{2}$, and $P_1 = A\left(\frac{1}{2Q} + \frac{z'}{Q}\right)$, $P_2 = A\left(\frac{1}{2Q} - \frac{z'}{Q}\right)$ Lemma 18 applies with $z = z'/Q$. Again we set $a_0 = c_0 = 1$ and $a_1 = a_2 = A, c_1 = \frac{1}{2Q} + z, c_2 = \frac{1}{2Q} - z$. By Lemma 16 $\Psi(\bar{\omega}, \bar{\lambda}, \bar{a} \cdot s, \bar{c}) \leq 3^{1-\gamma} - \delta$.
Case 3: $\left(1 - \frac{1}{Q}\right) \frac{1}{Q} \leq P_1 + P_2 \leq 1 - \frac{1}{Q}$. Let C be given by $\left(1 - \frac{1}{Q}\right) \cdot C = \frac{P_1 + P_2}{2}$. Then C is as required by Lemma 19. We have a $0 \leq z' \leq \frac{1}{2}$ such that

$$P_1 = \left(1 - \frac{1}{Q}\right) \cdot C \cdot 2\left(\frac{1}{2} + z'\right) = \left(1 - \frac{1}{Q}\right) \cdot (C + 2Cz'),$$
$$P_2 = \left(1 - \frac{1}{Q}\right) \cdot (C - 2Cz').$$

With $z = 2Cz' \leq C$ Lemma 19 applies. We set $a_0 = c_0 = 1$ and $a_1 = a_2 = 1 - 1/Q$ and $c_1 = C + z, c_2 = C - z$ and finish the argument as in Case 2.

Case 4: $P_1 + P_2 \geq 1 - \frac{1}{Q}$. With $A(x)$ as from Lemma 20 we have $A(x) \cdot x = \left(1 - \frac{7}{10Q}\right) x + \frac{7}{10Q} x^2$ and $A(x)x$ increases from 0 to 1 for $0 \leq x \leq 1$. Let y_i be such that $P_i = A(y_i) \cdot y_i$. Then $y_2 \leq y_1 \leq 1$ and we can represent y_i such that Lemma 20 is applicable.

$$y := \frac{y_1 + y_2}{2}, z := \frac{y_1 - y_2}{2}, \text{ and } y_1 = y + z, y_2 = y - z, z \leq y, 1 - y.$$

We show that $1 \geq y \geq 4/10$ and Lemma 20 applies to y, z. We have $P_1 + P_2 = A(y_1)y_1 + A(y_2)y_2 = y_1 + y_2 + 7/(10Q)(y_1^2 + y_2^2 - y_1 - y_2) \leq y_1 + y_2$. Therefore $y = (y_1 + y_2)/2 \geq 1/2(1 - 1/Q) \geq 4/10$ as $Q \geq s \geq 15$. Setting $a_0 = c_0 = 1, a_1 = A(y + z), a_2 = A(y - z), c_1 = y + z, c_2 = y - z$ implies the claim.

Now, assume the λ_i are ordered in a different way. We apply the permutation leading from $\lambda_0 \geq \lambda_1 \geq \lambda_2$ to the ordering considered to the P_i, a_i, c_i above. The first two factors of Ψ do not change, only $r(\bar{c})$ may change. But, Lemma 16 still applies. The three factors, OPT$_1$, OPT$_2$, OPT$_3$ of OPT$(\bar{a}, \bar{c}, s)$ do not change. This refers to C_1, and C_2, too, and the argument above for P_1 small applies, too. □

In the proofs to come in the following four subsections we use the notation

$$L(a,s) = \frac{q(as)}{q(s)} = \frac{\exp(as) - as - 1}{\exp(s) - s - 1}, \; K(a,s) = \frac{q'(as)}{q'(s)} = \frac{\exp(as) - 1}{\exp(s) - 1},$$
$$M(a,s) = \frac{\exp(as)}{\exp(s)}. \text{Then } aK(a,s) \leq L(a,s) \leq K(a,s) \leq M(a,s)\,, \; 0 \leq a \leq 1. \quad (7)$$

Proof of (7). $p(x) := q'(x)$, $K := K(a,s), L := L(a,s)$. For $a = 0$ or $a = 1$ we have $aK = L$. For $a > 0$, $aK \leq L \iff ap(as)/q(as) \leq p(s)/q(s) \iff asp(as)/q(as) \leq sp(s)/q(s)$. The preceding inequality holds trivially for $a = 1$. We show that $asp(as)/q(as)$ is strictly increasing in $a > 0$. We observe that $q(x)/(xp(x)) = 1/x - 1/p(x)$. The derivative is of the last expression is < 0 iff $x^2 + 2 < \exp(x) + 1/\exp(x)$. For $x = 0$ we have equality and several differentiations show the inequality.

For $a = 0, L \leq K$ is true. For $a > 0$ $L \leq K \iff 1 - sa/p(sa) \leq 1 - s/p(s)$. The last inequality follows from $a \geq p(sa)/p(s)$ for $0 \leq a \leq 1$. This follows from convexity. $K(a,s) \leq M(a,s)$ is very easy to show. □

$$\text{We also have } aK(a,s) \leq \frac{7}{10} L(a,s), \;\text{ for } 0 \leq a \leq \frac{1}{2}, s \geq 4 \;\text{ (proof omitted.)} \quad (8)$$

$$\text{We recall } Q(x) = \frac{xq'(x)}{q(x)} = \frac{x(\exp(x) - 1)}{\exp(x) - x - 1}, Q = Q(s) = k\gamma,\; Q(s) > s.$$

3.1 Proof of Lemma 17

Lemma 17 (repeated) Let $s \geq 8, A(x) = A(x,s) := (7/10)Q \cdot x$.
(a) OPT(y) := OPT $(1, A(y), A(y), 1, y, y, s)$ is strictly decreasing for $0 < y \leq 1/(2Q)$. The start value is OPT$(0) = 3$.
(b) Given $0 \leq y \leq 1/(2Q)$, OPT(z) := OPT$(1, A(y+z), A(y-z), 1, y+z, y-z, s)$ is decreasing in $0 \leq z \leq y$.
Proof of (a). We have

$$\text{OPT}(y) = (1 + 2L(A(y), s)) \left(\frac{1}{1 + 2A(y) \cdot y} \right)^Q \left((1 + 2y)^Q + 2(1 - y)^Q \right).$$

We write OPT$_1(y) = 1 + 2L(A(y), s)$. Clearly OPT$(0) = 3$.

We have $A' := \dfrac{d}{dy} A(y) = \dfrac{7}{10} Q$. And $\dfrac{d}{dy} \ln \text{ OPT } (y) >=< 0 \Longleftrightarrow$

$$\frac{A' \cdot 2 \cdot K(A(y), s)}{\text{OPT}_1(y)} - \frac{2A(y) + 2A' \cdot y}{1 + 2A(y) \cdot y} + \frac{2(1 + 2y)^{Q-1} - 2(1 - y)^{Q-1}}{(1 + 2y)^Q + 2(1 - y)^Q} >=< 0 \quad (9)$$

The relationship (9) is obtained by taking the derivative and dividing by Q. To get the first summand we look into the definition of Q (the formula after 8.)

$$\frac{d}{dy} \ln \text{ OPT }_1(y) = \frac{\frac{A's \cdot 2(\exp(A(y)s) - 1)}{q(s)}}{\text{OPT}_1(y)}, \frac{1}{Q(s)} \frac{A's \cdot 2(\exp(A(y)s) - 1)}{q(s)} = A' \cdot 2K(A(y), s)$$

Observe that the first and third term of (9) is ≥ 0 for $0 \leq y \leq 1$ whereas the second term is ≤ 0. Moreover, $A' \cdot y = A(y)$. We have that $\frac{d}{dy} \ln \text{ OPT } (y) < 0$ if the following two inequalities both hold:

$$\frac{A' \cdot 2 \cdot K(A(y), s)}{\text{OPT}_1(y)} < \frac{\frac{7}{10} A' \cdot y}{1 + 2A(y) \cdot y} \quad (10)$$

$$\frac{2(1 + 2y)^{Q-1} - 2(1 - y)^{Q-1}}{(1 + 2y)^Q + 2(1 - y)^Q} < \frac{\frac{33}{10} A' \cdot y}{1 + 2A(y) \cdot y} \quad (11)$$

Note that for $y = 0$ both sides of the first inequality are equal to 0 and of the second inequality, too. The derivative of OPT(y) is $= 0$ for $y = 0$.
Comment: It is important to split up the left-hand-side of inequality (9), otherwise the calculations get very complicated. Equally important is the step leading to (9). Analogous steps will occur several times.

Proof of (10) for $0 < y \le 1/(2Q)$, $s \ge 7$. We abbreviate $K := K(A(y), s)$, $L := L(A(y), s)$. Note $\mathrm{OPT}_1(y) = 1 + 2L$. As $A' > 0$ we show

$$\frac{2 \cdot K}{1 + 2L} < \frac{\frac{7}{10}y}{1 + 2A(y) \cdot y} \iff 2K + 4K \cdot A(y) \cdot y - 2\frac{7}{10}L \cdot y < \frac{7}{10}y.$$

$$\text{By (8) we know } K \cdot A(y) \le \frac{7}{10}L \text{ for } s \ge 4 \text{ as} A(y) \le \frac{1}{2} \text{ (by } y \le \frac{1}{2Q}.\text{)} \tag{12}$$

Thus (10) follows from $2K + 2K \cdot A(y) \cdot y < \frac{7}{10}y$. As $2K \cdot A(y) \cdot y \le 2K$ and $2K$ is convex and $2K = 0$ for $y = 0$ we show that $2K < (7/20)y$ for $y = 1/(2Q)$. For $y = 1/(2Q)$ we have $A(y) = 7/20$ and $2K = 2(\exp((7/20)s) - 1)/(\exp(s) - 1)$. As $1/(2Q) = (\exp(s) - s - 1)/(2s(\exp(s) - 1))$ we have for $y = 1/(2Q)$

$$2K < \frac{7}{20}y \iff 2\left(\exp\left(\frac{7}{20}s\right) - 1\right) < \frac{7}{40}\frac{\exp(s) - s - 1}{s}$$

This last inequality holds for $s \ge 7$ (but not for $s \le 4$.)

Proof of (11) for $y \le 1/Q$ *and* $s \ge 2$. Inequality (11) is equivalent to

$$2(1 + 2y)^{Q-1} - 2(1 - y)^{Q-1} <$$
$$< A(y)\left[\frac{33}{10}\left[(1 + 2y)^Q + 2(1 - y)^Q\right] - 2y \cdot \left[2(1 + 2y)^{Q-1} - 2(1 - y)^{Q-1}\right]\right] \tag{13}$$

The right-hand-side of (13) is $\ge$

$$A(y)\left[\frac{33}{10}\left[(1 + 2y)^Q + 2(1 - y)^Q\right] - \frac{33}{10}y \cdot \left[2(1 + 2y)^{Q-1} - 2(1 - y)^{Q-1}\right]\right]$$
$$= \frac{33}{10}A(y)\left[(1 + 2y)^{Q-1}(1 + 2y - 2y) + 2(1 - y)^{Q-1}(1 - y + y)\right]$$
$$= \frac{33}{10}A(y)\left[(1 + 2y)^{Q-1} + 2(1 - y)^{Q-1}\right].$$

$$\text{And (13) follows from } \frac{2(1 + 2y)^{Q-1} - 2(1 - y)^{Q-1}}{(1 + 2y)^{Q-1} + 2(1 - y)^{Q-1}} < \frac{33}{10}A(y) \tag{14}$$

For $y = 0$ both sides of (14) are equal to 0. We show that $33/10 \cdot A' >$ the derivative with respect to y of the left-hand-side of (14.) By elementary calculation

$$\frac{d}{dy}\frac{2(1+2y)^{Q-1} - 2(1-y)^{Q-1}}{(1+2y)^{Q-1} + 2(1-y)^{Q-1}} = \frac{18 \cdot (Q-1)(1+y-2y^2)^{Q-2}}{\left[(1+2y)^{Q-1} + 2(1-y)^{Q-1}\right]^2}.$$

We need to show $\dfrac{33}{10}\dfrac{7}{10}Q\left[(1+2y)^{Q-1} + 2(1-y)^{Q-1}\right]^2 > 18(Q-1)(1+y-2y^2)^{Q-2}$.

Enlarging the right-hand-side, $1 \leq 1+y-2y^2$ for $y \leq 1/Q \leq 1/s \leq 1/2$(by $Q(s) \geq s$)

we show $33 \cdot 7\left[(1+2y)^{Q-1} + 2(1-y)^{Q-1}\right]^2 > 1800(1+y-2y^2)^{Q-1}$

$$= 1800\left((1+2y)(1-y)\right)^{Q-1}$$

$$\Longleftrightarrow 231\left[(1+2y)^{2(Q-1)} + 4\left((1+2y)(1-y)\right)^{Q-1} + 4(1-y)^{2(Q-1)}\right] >$$

$$> 1800\left((1+2y)(1-y)\right)^{Q-1} \Longleftrightarrow \text{(Division by } \left((1+2y)(1-y)\right)^{Q-1}\text{)}$$

$$\Longleftrightarrow \left(\frac{1+2y}{1-y}\right)^{Q-1} + 4 + 4\left(\frac{1-y}{1+2y}\right)^{Q-1} > 1800/231.$$

Rescaling the fraction to x the preceding inequality follows from

$$x + 4\frac{1}{x} > 1800/231 - 4 = 3.79\ldots \text{ true for } x > 0.$$

Proof of (b). We assume $0 \leq y \leq 1/(2Q)$ and $0 < z \leq y$.

$$A(y+z) = \frac{7}{10}Q \cdot (y+z) \quad , \ A(y+z) \cdot (y+z) = \frac{7}{10}Q \cdot (y+z)^2$$

$$A(y+z) \cdot (y+z) + A(y-z) \cdot (y-z) = \frac{7}{10}Q \cdot 2(y^2+z^2)$$

$$\text{OPT}(z) = (1 + L(A(y+z), s) + L(A(y-z), s)) \cdot$$

$$\cdot \left(\frac{1}{1 + \frac{7}{10}Q \cdot 2(y^2+z^2)}\right)^Q \cdot \left((1+2y)^Q + 2 \cdot \left((1-y)^2 + 3z^2\right)^{Q/2}\right).$$

$$\frac{d}{dz}\ln \text{OPT}(z) > = < 0 \Longleftrightarrow$$

$$\frac{\frac{7}{10}Q \cdot K(A(y+z), s) - \frac{7}{10}Q \cdot K(A(y-z), s)}{1 + L(A(y+z), s) + L(A(y-z), s)} - \frac{\frac{7}{10}Q4z}{1 + \frac{7}{10}Q \cdot 2(y^2+z^2)} +$$

$$\frac{6z \cdot ((1-y)^2 + 3z^2)^{Q/2-1}}{(1+2y)^Q + 2 \cdot ((1-y)^2 + 3z^2)^{Q/2}} > = < 0.$$

The first term of the sum is obtained as the first term of (9.) The first and third term of the left-hand-side of the preceding inequality are ≥ 0 for $0 \leq z \leq y$ whereas the second term is ≤ 0.

Analogously to (10) and (11) $\frac{d}{dz}\ln \mathrm{OPT}(z) \, < \, 0$ is implied by

$$\frac{\frac{7}{10}Q\left[K(A(y+z),s) \, - \, K(A(y-z),s)\right]}{1 \, + \, L(A(y+z),s) \, + \, L(A(y-z),s)} \, < \, \frac{\frac{9}{10}\frac{28}{10}Qz}{1+\frac{14}{10}Q(y^2+z^2)} \tag{15}$$

$$\frac{6z\cdot((1-y)^2+3z^2)^{Q/2-1}}{(1+2y)^Q \, + \, 2\cdot((1-y)^2+3z^2)^{Q/2}} \, < \, \frac{\frac{1}{10}\frac{28}{10}Qz}{1+\frac{14}{10}Q(y^2+z^2)} \tag{16}$$

Proof of (15) for $y \le 1/(2Q)$ and $s \ge 3.5$. The denominator of the right-hand-side fraction is maximal for $y = z = 1/(2Q)$. In this case it is $1 + 7/(10Q) < 1 + 1/Q$. We lower the denominator of the left-hand-side simply to 1. The claim follows from

$$K(A(y+z),s) \, - \, K(A(y-z),s) \, < \, \frac{\frac{18}{5}z}{1+\frac{1}{Q}}$$

The left-hand-side of the preceding inequality is convex in z for all $y < 1/(2Q)$ (based on the convexity of $\exp(x) - \exp(-x)$.) For $z = 0$ both sides are $= 0$. Therefore it is sufficient to show that the inequality holds for $z = y$ where $y \le 1/(2Q)$. Setting $z = y$ yields $K(A(y-z),s) = 0$ and we show

$$K(A(2y),s) \, < \, \frac{\frac{18}{5}y}{1+\frac{1}{Q}}$$

Again by convexity of the left-hand-side it is sufficient to show the inequality for $y = 1/(2Q)$. In this case we need to show

$$K(A(1/Q),s) \, = \, \frac{\exp\left(\frac{7}{10}s\right)-1}{\exp(s)-1} \, < \, \frac{18}{10}\frac{1}{Q+1}$$

By (7) we know $\frac{\exp\left(\frac{7}{10}s\right)-1}{\exp(s)-1} \, \le \, \exp\left(-\frac{3}{10}s\right)$.

And $\exp\left(-\frac{3}{10}s\right) \, < \, \frac{18}{10}\frac{1}{Q+1}$ holds (proof omitted) for $s \ge 3.5$.

Proof of (16) for $s \ge 8$. We show

$$\frac{(1+2y)^Q \, + \, 2\cdot((1-y)^2+3z^2)^{Q/2}}{6z\cdot((1-y)^2+3z^2)^{Q/2-1}} \, > \, \frac{1+\frac{14}{10}Q(y^2+z^2)}{\frac{1}{10}\frac{28}{10}Qz}.$$

Canceling z in the denominator , setting $z = y$ on the right-hand-side, this follows from

$$\frac{(1+2y)^Q}{6\cdot((1-y)^2+3z^2)^{Q/2-1}} \, + \, \frac{1}{3}((1-y)^2+3z^2) \, > \, \frac{1+\frac{14}{5}Qy^2}{\frac{28}{100}Q} \, = \, \frac{100}{28Q}+10y^2$$

As $(1-y)^2+3z^2 \, \le \, 1-2y+4y^2 \, < 1$ by $y \le 1/(2Q), Q \ge s \ge 8$

this follows from $\frac{1}{6}(1+2y)^Q \, + \, \frac{1}{3}(1-y)^2 \, > \, \frac{100}{28Q}+10y^2$

The last inequality holds for $Q \geq 8, y \geq 0$ and then the claim holds as $Q \geq s$.

3.2 Proof of Lemma 18

Lemma 18 (repeated) Let $s \geq 7$ and $\frac{7}{20} \leq A \leq 1 - \frac{1}{Q}$. Then
$\mathrm{OPT}(z) := \mathrm{OPT}(1, A, A, 1, 1/(2Q) + z, 1/(2Q) - z, s) \leq 3 - \delta$ for $0 \leq z \leq 1/(2Q)$.

Proof. $\mathrm{OPT}(z) =$

$$(1 + 2 \cdot L(A,s)) \left(\frac{1}{1+\frac{A}{Q}}\right)^Q \cdot \left[\left(1+\frac{1}{Q}\right)^Q + 2\left(\left(1-\frac{1}{2Q}\right)^2 + 3z^2\right)^{1/2 \cdot Q}\right]$$

is increasing in z. We show the claim for $z = 1/(2Q)$. Let from now on $\mathrm{OPT}(A) = \mathrm{OPT}(1, A, A, 1, 1/Q, 0, s) =$

$$(1 + 2 \cdot L(A,s)) \left(\frac{1}{1+\frac{A}{Q}}\right)^Q \cdot \left[\left(1+\frac{1}{Q}\right)^Q + 2\left(1-\frac{1}{Q}+\frac{1}{Q^2}\right)^{1/2 \cdot Q}\right]$$

First, we show that $\mathrm{OPT}(A)$ has exactly one extremum in $0 \leq A \leq 1$ which is a minimum.

$$\frac{d}{dA} \ln \mathrm{OPT}(A) >=< 0 \Longleftrightarrow \frac{2K(A,s)}{1+2L(A,s)} - \frac{\frac{1}{Q}}{1+\frac{A}{Q}} >=< 0.$$

Concerning the first term of the preceding sum we refer to the explanation following (9.) For $A = 0$ the first term is $= 0$ and the derivative is < 0. For $A = 1$ the first term is $= 2/3$, whereas the second term is $1/(Q+1) < 2/3$ for $Q > s > 2$, and the derivative is > 0. We show that the derivative is $= 0$ for exactly one $0 < A < 1$ which must be a minimum.

The second fraction of the derivative is decreasing in A. We check that the first fraction is increasing. Abbreviating $L = L(A,s)$, $L' = \frac{d}{dA} L(A,s)$ and analogously for K, we get

$$\frac{d}{dA}\frac{2K(A,s)}{1+2L(A,s)} > 0 \Longleftrightarrow 2K'(1+2L) > 2K2L' \Longleftrightarrow$$

(Multiplication with $(\exp(s) - s - 1)(\exp(s) - 1)$, division by 2 and s.)

$$(\exp(s) - s - 1)\exp(sA) + \exp(sA)2(\exp(sA) - sA - 1) > 2(\exp(sA) - 1)^2$$

$$\Longleftrightarrow (\exp(s) - s - 2sA)\exp(sA) > -\exp(sA) + 2$$

$$\Longleftrightarrow \exp(s) - s - 2sA > -1 + 2/\exp(sA)$$

which is true for $s > 2, 0 < A < 1$ by convexity of $2/\exp(sA)$.

We need to show the claim for the boundary values $A = 7/20$ and $A = 1 - 1/Q$. First, $A = 7/20$:

$$1 \,+\, 2L(A,s) \,\leq 1 + 2M(A,s) \,=\, 1 \,+\, 2\exp(-13/20 \cdot s) \quad \text{(by (7).)}$$

With the derivative of the logarithm and the Mean Value Theorem we can show that $\left(\frac{1+\frac{1}{Q}}{1+\frac{A}{Q}}\right)^{Q}$ is increasing in Q towards its limit $\exp(13/20)$. $\frac{2\left(1-\frac{1}{Q}\,+\,\frac{1}{Q^2}\right)^{1/2\cdot Q}}{\left(1+\frac{A}{Q}\right)^{Q}}$ is decreasing in $Q = Q(s) \geq 2$ (proof by standard calculus methods) and therefore also in s towards its limit $2\exp(-17/20)$. For $Q = 7$ we get a value ≤ 0.9 Therefore, for all $\geq s\, \geq 7($ as $Q(s) \geq s)$

$$\text{OPT}(A) \,<\, (1 + \,2\exp(-13/20 \cdot 7))(\exp(13/20) + 0.9) \,=\, 2.87\ldots\,.$$

Now, $A = 1 - 1/Q$:

$$1 \,+\, 2L(A,s) \,\leq\, 1 \,+\, 2M(A,s) \,=\, 1 \,+\, 2\exp\left(-\frac{s}{Q}\right)$$

$$=\, 1 + 2\exp\left(-\frac{\exp(s) - s - 1}{\exp(s) - 1}\right) \text{ decreasing in } s \text{ to } 1 + 2\exp(-1).$$

For $s = 7$ we get $1 + 2L(A,s) \leq 1.7404\ldots$

$$\left(\frac{1+\frac{1}{Q}}{1+\frac{A}{Q}}\right)^{Q} \;=\; \left(\frac{1+\frac{1}{Q}}{1\,+\,\frac{1}{Q}\,-\,\frac{1}{Q^2}}\right)^{Q} \text{ is decreasing in } Q = Q(s)$$

(elementary proof omitted) and therefore in s to 1. For $Q = 7$ we get $1.1344\ldots$. As $Q(s) \geq s$ this bound applies to $s = 7$, too.

$$\frac{2\left(1-\frac{1}{Q}+\frac{1}{Q^2}\right)^{1/2\cdot Q}}{\left(1+\frac{1}{Q}-\frac{1}{Q^2}\right)^{Q}} \text{is again decreasing (proof omitted) in}$$

Q and s to $2\exp(-3/2)$. For $Q = 7$ we get $0.564\ldots$

Altogether for $Q(s) \geq s \geq 7$

$$\text{OPT}(A) \leq 1.741 \cdot (1.135 + 0.565) \,=\, 2.9597.$$

3.3 Proof of Lemma 19

Lemma 19 (repeated) Let $s \,\geq\, 7$ and $1/(2Q) \leq C \leq 1/2$. Then
$\text{OPT}(z) := \text{OPT}(1, 1 - 1/Q,\, 1 - 1/Q,\, 1, C + z,\, C - z\,, s) \,\leq 3\, -\, \delta$ for $0 \leq z \leq C$.

Proof. We abbreviate $A = 1 - 1/Q$. First, analogously to the proof of Lemma 18 we can restrict attention to $z = C$. OPT(z) $=$

$$= (1 + 2L(A, s)) \left(\frac{1}{1 + 2AC}\right)^{Q} \left[(1 + 2C)^{Q} + 2((1 - C)^{2} + 3z^{2})^{1/2 \cdot Q}\right]$$

Let from now on OPT(C) $=$ OPT$(1, A, A, 1, 2C, 0, s)$ $=$

$$= (1 + 2L(A, s)) \left(\frac{1}{1 + 2AC}\right)^{Q} \cdot \left[(1 + 2C)^{Q} + 2(1 + 4C^{2} - 2C)^{1/2 \cdot Q}\right]$$

OPT(C) has exactly one extremum, which is a minimum for $0 \leq C \leq 1$.

$$\frac{d}{dc} \ln \text{OPT}(C) >=< 0 \Longleftrightarrow$$

$$-\frac{2A}{1 + 2AC} + \frac{2(1 + 2C)^{Q-1} + (8C - 2)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1}}{(1 + 2C)^{Q} + 2(1 + 4C^{2} - 2C)^{1/2 \cdot Q}} >=< 0 \Longleftrightarrow$$

$$2A \left((1 + 2C)^{Q} + 2(1 + 4C^{2} - 2C)^{1/2Q}\right) -$$

$$- 2AC \left(2(1 + 2C)^{Q-1} + (8C - 2)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1}\right) =$$

$$= 2A \left[(1 + 2C)^{Q-1} + (2 - 2C)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1}\right] < = >$$

$$< = > 2(1 + 2C)^{Q-1} + (8C - 2)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1} \Longleftrightarrow$$

$$2A < = > \frac{2(1 + 2C)^{Q-1} + (8C - 2)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1}}{(1 + 2C)^{Q-1} + (2 - 2C)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1}} \Longleftrightarrow$$

$$A < = > \frac{(1 + 2C)^{Q-1} + (4C - 1)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1}}{(1 + 2C)^{Q-1} + (2 - 2C)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1}}$$

For $C = 0$ the right-hand-side fraction is equal to $0 < A$ and OPT(C) is decreasing. For $C = 1$ the right-hand-side fraction is greater than $1 > A$ and OPT(C) is increasing.

Next we show that the preceding fraction is increasing in $0 < C < 1$, and equality is attained for only one C which must be a minimum.

Rewriting $4C - 1 = (2 - 2C) + 6C - 3$ the fraction is rewritten as

$$1 + \frac{(6C - 3)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1}}{(1 + 2C)^{Q-1} + (2 - 2C)(1 + 4C^{2} - 2C)^{1/2 \cdot Q - 1}}$$

Rescaling $1/2 \cdot Q - 1$ to Q (then $Q - 1$ scales to $2Q + 1$) and $2C$ to C we get

$$1 + \frac{(3C - 3)(1 + C^{2} - C)^{Q}}{(1 + C)^{2Q+1} + (2 - C)(1 + C^{2} - C)^{Q}}$$

Dividing through $3(C - 1)(1 + C^{2} - C)^{Q}$ the preceding fraction is certainly increasing if $\frac{(1 + C)^{2Q+1}}{3(C - 1)(1 + C^{2} - C)^{Q}}$ and $\frac{2 - C}{3(C - 1)}$ are both decreasing for $0 < C < 2, C \neq 1$.

The second fraction is easily seen to be decreasing. We show that the inverse of the first fraction is increasing. The numerator of its derivative is

$$\begin{aligned} &\big[(1+C^2-C)^Q + (C-1)(2C-1)Q(1+C^2-C)^{Q-1}\big] \cdot (1+C)^{2Q+1} \; - \\ &- (C-1)(1+C^2-C)^Q \cdot (2Q+1)(1+C)^{2Q} \; = \; (1+C)^{2Q}(1+C^2-C)^{Q-1} \cdot \\ &\big[(1+C)(1+C^2-C) \; + \; (1+C)(C-1)(2C-1)Q \; - \; (2Q+1)(C-1)(1+C^2-C)\big] \end{aligned}$$

The expression in square brackets can be rewritten as

$$\begin{aligned} &(1+C)(C-1)(2C-1)Q \; - \; 2Q(C-1)(1+C^2-C) \; + \; (-C+1+C+1)(1+C^2-C) \\ &= \; Q(1-C)^2 \; + \; 2(1+C^2-C) \; > \; 0 \end{aligned}$$

Now it is sufficient to show the claim for the boundary values, $C = 1/(2Q)$ and $C = 1/2$. The first case is contained in Lemma 18. Let $C = 1/2$. We proceed as in the proof of Lemma 18, case $A = 1 - 1/Q$.

$1 + 2L(A,s) \leq 1.7404$ for $s \geq 7$

$$\left(\frac{1+2C}{1\,+\,2CA}\right)^Q \;=\; \left(\frac{2}{2\,-\,\frac{1}{Q}}\right)^Q$$ is decreasing in $Q = Q(s)$

(elementary proof omitted) and therefore in s to $\exp(-1/2)$.

For $Q = 7$ we get $1.67993\ldots$. As $Q(s) \geq s$ this bound applies to $s = 7$, too.

$$\frac{2(1+4C^2-2C)^{1/2\cdot Q}}{(1+2AC)^Q} \;=\; \frac{2}{(2-\frac{1}{Q})^Q}$$ decreasing to 0

For $Q = 7$ we get $0.02624\ldots$

Altogether OPT$(C) \leq 1.75 \cdot (1.68 + 0.027) = 2.98$ for $s \geq 7$.

3.4 Proof of Lemma 20

Lemma 20 (repeated) Let $s \geq 15$ and $A(x) \;=\; A(x,s) \;:=\; 1 + 7/(10Q) \cdot x \,-\, 7/(10Q)$.
(a) OPT(y) :=OPT$(1, A(y), A(y), 1, y, y, s)$ is strictly increasing in $4/10 \leq y < 1$. The final value is OPT$(1) = 3$.
(b) Given $4/10 \leq y \leq 1$, OPT(z) :=OPT$(1, A(y+z), A(y-z), 1, y+z, y-z, s)$ is decreasing in $0 \leq z \leq \min\{y, 1-y\}$.

Proof of (a). We have $\text{OPT}(y) \ =$

$$(1+2L(A(y),s))\left(\frac{1}{1+2A(y)\cdot y}\right)^{Q}\left((1\ +\ 2y)^{Q}\ +\ 2\,(1\ -\ y)^{Q}\right)$$

We write $\text{OPT}_1(y) = 1+2L(A(y),s)$. Clearly $\text{OPT}(1) \ = \ 3$

We have $A' := \dfrac{d}{dy}A(y) \ = \ \dfrac{7}{10}\dfrac{1}{Q}$.

$$\frac{d}{dy}\ln\ \text{OPT}\ (y)\ >=<\ 0 \iff \text{(See comment to (9.))}$$

$$\frac{A'\cdot 2\cdot K(A(y),s)}{\text{OPT}_1(y)} - \frac{2A(y)\ +\ 2A'\cdot y}{1+2A(y)\cdot y} + \frac{2(1+2y)^{Q-1}-2(1-y)^{Q-1}}{(1\ +\ 2y)^{Q}\ +\ 2\,(1\ -\ y)^{Q}}\ >=<\ 0$$

Observe that the first and third term of the preceding sum are ≥ 0 for $0 \leq y \leq 1$ whereas the second term is ≤ 0.

We have that $\frac{d}{dy}\ln\ \text{OPT}\ (y) > 0$ if the following two inequalities both hold:

$$\frac{A'\cdot 2\cdot K(A(y),s)}{\text{OPT}_1(y)} > \frac{2A'\cdot y}{1+2A(y)\cdot y} \tag{17}$$

$$\frac{2(1+2y)^{Q-1}-2(1-y)^{Q-1}}{(1\ +\ 2y)^{Q}\ +\ 2\,(1\ -\ y)^{Q}} > \frac{2A(y)}{1+2A(y)\cdot y} \tag{18}$$

Note that for $y=1$ both sides of the first inequality are equal to $7/(10Q)\cdot 2/3$ and of the second inequality $2/3$. Therefore the derivative of $\text{OPT}(y)$ is $=0$ for $y=1$.

Proof of (17) for $1 > y \geq \ 0\ ,\ \ s \geq 4$. Let $K = K(A(y),s)$ and $L = L(A(y),s)$.

As $A' > 0$ we need to show $\dfrac{K}{1+2L}\ >\ \dfrac{y}{1+2A(y)\cdot y}$.

$$\iff K\ +\ 2K\cdot A(y)y\ -\ 2L\cdot y\ >\ y$$

As $K \geq L$ by (7) this follows from

$$K\,(1\ +\ 2A(y)\cdot y\ -2y)\ \ =\ K\left(1+2\frac{7}{10Q}y^{2}-2\frac{7}{10Q}y)\right)\ >\ y \tag{19}$$

For $y=1$ both sides of (19) are $=1$. For $y=0$ (19) holds as $K>0$ in this case.

K considered as a function in y is convex, increasing and >0. The second term on the left-hand-side of (19), $1-2\frac{7}{10Q}y^2+2\frac{7}{10Q}y$, is convex, >0, and increasing for $y>1/2$. Therefore the left-hand-side of (19) is convex for $1/2 < y < 1$. We next show that the derivative of the left-hand-side at $y=1$ is <1. This implies that (19) holds for $1/2 \leq y < 1$.

$$\frac{d}{dy}K\left(1\ +\ 2\frac{7}{10Q}y^2\ -\ 2\frac{7}{10Q}y)\right)\ =\ \frac{s\cdot\frac{7}{10Q}\cdot\exp(sA(y))}{\exp(s)-1}$$
$$\cdot\left(1\ \ +2\frac{7}{10Q}y^2\ -\ 2\frac{7}{10Q}y\right)\ +\ \frac{\exp(sA(y))-1}{\exp(s)-1}\cdot\left(4\frac{7}{10Q}y\ -\ 2\frac{7}{10Q}\right).$$
$$\text{Plugging in }\ y=1\ \text{ yields }\frac{7}{10Q}\left(\frac{s\exp(s)}{\exp(s)-1}+2\right)\tag{20}$$

For $s=4$ (20) is $0.9837\dots<1$. As (20) is in decreasing in s (proof omitted) (19) holds for all $s\geq 4$ and $1/2\leq y<1$.

$1-2\frac{7}{10Q}y^2+2\frac{7}{10Q}y$ is decreasing for $y<1/2$. Therefore, for $0\leq y\leq 1/2$, we can bound the left-hand-side of (19) from below by

$$K\left[\left(1+2\frac{7}{10Q}y^2-2\frac{7}{10Q}y\right)_{y=1/2}\right]$$

This function (the argument y occurs only in K) is convex in y . For $y=1/2$ it is $>y$ by the previous argument. For $y=1$ it is $<y$. Therefore it is $>y$ for $0\leq y\leq 1/2$. The claim is shown.

Proof of (18) for $y\geq 4/10$ *and* $s\geq 3.5$. Inequality (18) is equivalent to

$$2(1+2y)^{Q-1}-2(1-y)^{Q-1}\ >$$
$$>2A(y)\left[(1\ +\ 2y)^Q\ +\ 2\,(1\ -\ y)^Q\ -\ y\cdot\left[2(1+2y)^{Q-1}-2(1-y)^{Q-1}\right]\right]\ =$$
$$=\ 2A(y)\left[(1+2y)^{Q-1}(1+2y-2y)\ +\ 2(1-y)^{Q-1}(1-y+y)\right)$$
$$=\ 2A(y)\left[(1+2y)^{Q-1}+2(1-y)^{Q-1}\right]\iff\frac{(1+2y)^{Q-1}-(1-y)^{Q-1}}{(1+2y)^{Q-1}+2(1-y)^{Q-1}}\ >\ A(y)\tag{21}$$

For $y=1$ both sides of (21) are equal to 1. For $y<1$ (21) can be rewritten as

$$\left(\frac{1+2y}{1-y}\right)^{Q-1}\ >\ \frac{2A(y)+1}{1-A(y)}.\text{ With }y=\frac{4}{10}\text{ this becomes }3^{Q-1}\ >\ \frac{30}{7}Q\ -\ 2.$$

The preceding inequality holds for $Q>s\geq 3.5$. and we have the claim for $y=4/10$.

To show the claim for $4/10<y<1$ we show that the left-hand-side of (21) is concave in y. The derivative of the left-hand-side is

$$9(Q-1)\frac{(1+y-2y^2)^{Q-2}}{[(1+2y)^{Q-1}\ +\ 2(1-y)^{Q-1}]^2}$$

This is a decreasing function in $y \geq 4/10$ because the numerator is decreasing in this case whereas the denominator is increasing and > 0.

Proof of (b). Some preparatory calculations:

$$A(y+z) \;=\; A(y) \;+\; \frac{7}{10Q}z \;, \quad A(y-z) \;=\; A(y) \;-\; \frac{7}{10Q}z$$

$$A(y+z)\cdot(y+z) \;=\; A(y)y + A(y)z + \frac{7}{10Q}zy + \frac{7}{10Q}z^2$$

$$A(y-z)\cdot(y-z) \;=\; A(y)y - A(y)z - \frac{7}{10Q}zy + \frac{7}{10Q}z^2$$

$$A(y+z)\cdot(y+z) \;+\; A(y-z)\cdot(y-z) \;\;=\; 2A(y)\cdot y + \frac{14}{10Q}z^2$$

We denote

$$\text{OPT}_1(z) \;=\; 1 \;+\; L(A(y+z),s) \;+\; L(A(y-z),s)$$

$$\text{Then OPT}(z) \;=\; \text{OPT}_1(z)\,\cdot$$

$$\cdot \left(\frac{1}{1+2A(y)\cdot y + \frac{14}{10Q}z^2}\right)^Q \cdot \left((1+y)^Q \;+\; 2\cdot\left((1-y)^2 \;+\; 3z^2\right)^{Q/2}\right).$$

We proceed to show that $\frac{d}{dz}\ln \text{OPT}(z) \;<\; 0$ for $z > 0$. Some derivatives first.

$$\frac{d}{dz}\,A(y+z) \;=\; \frac{7}{10}\frac{1}{Q}, \qquad \frac{d}{dz}\,A(y-z) \;=\; -\frac{7}{10}\frac{1}{Q},$$

$$\frac{d}{dz}\left(1+2A(y)\cdot y + \frac{14}{10Q}z^2\right) \;=\; \frac{28}{10Q}z$$

$$\frac{d}{dz}\left((1+y)^Q \;+\; 2\cdot((1-y)^2+3z^2)^{Q/2}\right) \;=\; 6z\cdot Q\cdot((1-y)^2+3z^2)^{Q/2-1}.$$

$$\frac{d}{dz}\ln \text{OPT}(z) \;>=<\; 0 \iff \text{(Recall comment to (9).)}$$

$$\frac{\frac{7}{10Q}K(A(y+z),s) \;-\; \frac{7}{10Q}K(A(y-z),s)}{\text{OPT}_1(z)} \;-\; \frac{\frac{28}{10Q}z}{1+2yA(y)+\frac{14}{10Q}z^2} \;+$$

$$\frac{6z\cdot((1-y)^2+3z^2)^{Q/2-1}}{(1+y)^Q \;+\; 2\cdot((1-y)^2+3z^2)^{Q/2}} \;\; >=< \;\; 0.$$

Observe that the first and third term of the preceding inequality are $\geq\; 0$ for $0 \;\leq\; z \;\leq\; \min\{y, 1-y\}$, whereas the second term is ≤ 0.

We have that $\frac{d}{dz} \ln$ OPT $(z) < 0$ if the following two inequalities both hold:

$$\frac{\frac{7}{10Q}\left(K(A(y+z),s) \,-\, K(A(y-z),s)\right)}{\mathrm{OPT}_1(z)} \;<\; \frac{\frac{11}{10Q}z}{1+2yA(y)+\frac{14}{10Q}z^2} \tag{22}$$

$$\frac{6z\cdot((1-y)^2+3z^2)^{Q/2-1}}{(1+y)^Q \,+\, 2\cdot((1-y)^2+3z^2)^{Q/2}} \;<\; \frac{\frac{17}{10Q}z}{1+2yA(y)+\frac{14}{10Q}z^2} \tag{23}$$

Note that for $z = 0$ both sides of the preceding inequalities are equal to 0 and the derivative of $\ln \mathrm{OPT}(z)$ is $= 0$. Moreover, we have $1+2yA(y)+\frac{14}{10Q}z^2 \;\leq\; 1+2y$ and the inequalities follow when they are shown with the denominator $1+2y$ in the right-hand-side fraction. To get this, observe that

$$2yA(y) + \frac{14}{10Q}z^2 \;=\; 2y + \frac{14}{10Q}\left(y^2 - y + z^2\right) \leq 2y,$$

as $z \leq \min\{y, 1-y\}$ we have $z^2 \leq y(1-y)$ or $y(y-1)+z^2 \leq 0$.

Proof of (22) for $0 < z < \min\{y, 1-y\}, 0 \leq y \leq 1, s \geq 5$. We enlarge the left-hand-side of (22) first:

$$\begin{aligned}K(A(y+z),s) \,-\, K(A(y-z),s) \;&=\; \frac{1}{\exp(s)-1}\left(\exp(A(y+z)\cdot s) \,-\, \exp(A(y-z)\cdot s)\right)\\ &=\; \frac{\exp(A(y)s)}{\exp(s)-1}\left[\exp\left(\frac{7}{10Q}sz\right) \,-\, \exp\left(-\frac{7}{10Q}sz\right)\right]\end{aligned}$$

$$\begin{aligned}\mathrm{OPT}_1(z) \;&=\; 1 \,+\, L(A(y+z),s) \,+\, L(A(y-z),s) \;\;=\; 1 + \frac{1}{\exp(s)-s-1}\cdot\\ &\cdot[\exp(A(y+z)s) \,-\, A(y+z)s \,-1 \,+\, \exp(A(y-z)s) \,-\, A(y-z)s \,-1]\\ &\geq \text{ (As } A(y+z), A(y-z) \leq 1.)\\ 1 \;+\; \frac{1}{\exp(s)-1}&[\exp(A(y+z)s) \,+\, \exp(A(y-z)s) \,-\, 2s \,-2] \;=\; \frac{1}{\exp(s)-1}\cdot\\ &\cdot\left[\exp(s) \,-2s \,-3 \,+\, \exp(A(y)s)\left(\exp\left(\frac{7}{10Q}sz\right) \,+\, \exp\left(-\frac{7}{10Q}sz\right)\right)\right]\\ &\geq \text{ (As } A(y)s \leq s \text{ and } s \geq 2 \text{ so that } \exp(s)-2s-3 > 0.)\\ \frac{\exp(A(y)s)}{\exp(s)-1}&\left[\frac{\exp(s) \,-2s \,-3}{\exp(s)} \,+\, \exp\left(\frac{7}{10Q}sz\right) \,+\, \exp\left(-\frac{7}{10Q}sz\right)\right]\\ &\geq\; \frac{\exp(A(y)s)}{\exp(s)-1}\left[0.9 \,+\, \exp\left(\frac{7}{10Q}sz\right) \,+\, \exp\left(-\frac{7}{10Q}sz\right)\right],\end{aligned}$$

as $(\exp(s) - 2s - 3)/\exp(s) \geq 0.9$ for $s \geq 5$. The denominator of the right-hand-side of (22) is enlarged by $1 + 2y \leq 3$. We set

$$u = \exp\left(\frac{7}{10Q}sz\right) > 1 \text{ and show (simple algebra from (22)) } \frac{u - \frac{1}{u}}{0.9 + u + \frac{1}{u}} < \frac{11}{3 \cdot 7}z$$

$$\text{We have } z = (\ln u)\frac{10}{7}\frac{Q}{s} > (\ln u)\frac{10}{7} \text{ (by } Q > s.)$$

$$\text{Therefore it is enough to show } \frac{u - \frac{1}{u}}{0.9 + u + \frac{1}{u}} < (\ln u)\frac{10}{7}\frac{11}{21}$$

Elementary means show that this is true for $u > 1$.

Proof of (23) for $s \geq 15, 1 \geq y \geq 2/10$, $0 < z \leq \min\{y, 1 - y\}$. Inequality (23) follows from

$$\begin{aligned} \frac{6z \cdot ((1-y)^2 + 3z^2)^{Q/2-1}}{(1+y)^Q} &< \frac{\frac{17}{10Q}z}{1+2y} \\ \Longleftrightarrow 60Q(1+2y)((1-y)^2 + 3z^2)^{Q/2-1} &< 17(1+y)^Q \end{aligned} \tag{24}$$

For $y \leq 1/2$ we have $z \leq y$ and (24) follows from

$$60Q(1+2y)(1 - 2y + 4y^2)^{Q/2-1} < 17(1+y)^Q$$

The preceding inequality holds for $Q \geq s \geq 15$ and $1/2 \geq y \geq 2/10$ (proof omitted.)

For $y \geq 1/2$ we have $z \leq 1 - y$ and (24) follows from

$$60Q(1+2y)(4(1-y)^2)^{Q/2-1} < 17(1+y)^Q$$

This inequality holds for $Q \geq s \geq 10$ and $y \geq 1/2$ (details omitted.)

4 Proof of Lemma 13 and Theorem 15

We consider $\Psi(\bar{\omega}\,,\,\bar{\lambda})\,=\,\Psi(\bar{\omega}\,,\,\bar{\lambda}\,,\,\bar{a}\,,\,\bar{c}\,)$ as function of w_i, λ_i, $i = 1,2$ in a neighborhood of $(\omega_1,\omega_2) = (\lambda_1,\lambda_2) = (1/3,1/3)$. The parameters a_i, c_i are given by $Q(a_i) = \lambda_i k\gamma/\omega_i$, and $c_0 = 1$, $\;R(c_1,c_2) = (\lambda_1 k, \lambda_2 k)$. Subsection 5.1 shows that this is well defined and a_i, c_i is differentiable in λ_i, ω_i. For $\lambda_i = 1/3, \omega_i = 1/3$ we have $a_i = s, c_i = 1$ $(Q(s) = k\gamma$ defining s.) We show that the partial derivatives of $\ln\Psi(\bar{\omega}\,,\,\bar{\lambda})$ are 0 for $\omega_i = \lambda_i = 1/3$ and the Hessian matrix is negative definite. This implies Lemma 13.

For $i = 1,2$ the first derivatives are, with a_i', c_i' denoting the right derivatives of a_i, c_i resp. and recalling that $Q(x) = \frac{xq'(x)}{q(x)}$, $q(x) = \exp(x) - x - 1$, $R(x_1,x_2) = \left(\frac{x_1 r_{x_1}(1,x_1,x_2)}{r(1,x_1,x_2)}\,,\,\frac{x_2 r_{x_2}(1,x_1,x_2)}{r(1,x_1,x_2)}\right)$

$$\begin{aligned}
\frac{d\ln\Psi(\bar{\omega},\bar{\lambda})}{d\omega_i} &= -\ln q(a_0) + \omega_0\frac{a_0' q'(a_0)}{q(a_0)} + \ln\omega_0 + 1 + \\
&\qquad + \ln q(a_i) + \omega_i\frac{a_i' q'(a_i)}{q(a_i)} - \ln\omega_i - 1 - \\
&\qquad -k\gamma\lambda_0\frac{a_0'}{a_0} - k\gamma\lambda_i\frac{a_i'}{a_i} \\
&= \ln\omega_0 - \ln\omega_i + \ln q(a_i) - \ln q(a_0) \quad (\text{ using } Q(a_i) = k\gamma\lambda_i/\omega_i).
\end{aligned} \tag{25}$$

$$\begin{aligned}
\frac{d\ln\Psi(\bar{\omega},\bar{\lambda})}{d\lambda_i} &= \omega_0\frac{a_0' q'(a_0)}{q(a_0)} + \omega_i\frac{a_i' q'(a_i)}{q(a_i)} + \\
&\qquad k\gamma\Bigg(- \ln\lambda_0 - 1 + \ln a_0 - \lambda_0\frac{a_0'}{a_0} + \\
&\qquad\quad + \ln\lambda_i + 1 - \ln a_i - \lambda_i\frac{a_i'}{a_i} - \\
&\qquad\quad - \ln c_i - \lambda_1\frac{c_1'}{c_1} - \lambda_2\frac{c_2'}{c_2}\Bigg) + \\
&\qquad \gamma\frac{c_1' r_{c_1}(1,c_1,c_2) + c_2' r_{c_2}(1,c_1,c_2)}{r(1,c_1,c_2)} \\
&= k\gamma(\ln\lambda_i - \ln\lambda_0 + \ln a_0 - \ln a_i - \ln c_i) \\
&\qquad (\text{ using } \; R(c_1,c_2) = (k\lambda_1, k\lambda_2), Q(a_i) = k\gamma\lambda_i/\omega_i))
\end{aligned} \tag{26}$$

For $\bar{\lambda} = \bar{\omega} = (1/3,1/3)$ the terms in (25) and (26) yield 0.

The second derivatives (with $i, j \in \{1, 2\}, i \neq j)$ are (observe that some of the subsequent terms are equal as the derivative does not depend on the ordering of the variables)

$$\frac{d^2 \ln \Psi(\bar{\omega}, \bar{\lambda})}{d\lambda_i, \lambda_i} = k\gamma \left(\frac{1}{\lambda_i} + \frac{1}{\lambda_0} + \frac{a_0'}{a_0} - \frac{a_i'}{a_i} - \frac{c_i'}{c_i} \right) \tag{27}$$

$$\frac{d^2}{d\lambda_i, \lambda_j} = k\gamma \left(\frac{1}{\lambda_0} + \frac{a_0'}{a_0} - \frac{c_i'}{c_i} \right) \tag{28}$$

$$\frac{d^2 \ln \Psi(\bar{\omega}, \bar{\lambda})}{d\omega_i, \omega_i} = -\frac{1}{\omega_0} - \frac{1}{\omega_i} + \frac{a_i' q'(a_i)}{q(a_i)} - \frac{a_0' q'(a_0)}{q(a_0)} \tag{29}$$

$$\frac{d^2 \ln \Psi(\bar{\omega}, \bar{\lambda})}{d\omega_i, \omega_j} = -\frac{1}{\omega_0} - \frac{a_0' q'(a_0)}{q(a_0)} \tag{30}$$

$$\frac{d^2 \ln \Psi(\bar{\omega}, \bar{\lambda})}{d\omega_i, \lambda_i} = \frac{a_i' q'(a_i)}{q(a_i)} - \frac{a_0' q'(a_0)}{q(a_0)} \tag{31}$$

$$\frac{d^2}{d\omega_i, \lambda_j} = -\frac{a_0' q'(a_0)}{q(a_0)} \tag{32}$$

$$\frac{d^2 \ln \Psi(\bar{\omega}, \bar{\lambda})}{d\lambda_i, \omega_i} = k\gamma \left(\frac{a_0'}{a_0} - \frac{a_i'}{a_i} \right) \tag{33}$$

$$\frac{d^2 \ln \Psi(\bar{\omega}, \bar{\lambda})}{d\lambda_i, \omega_j} = k\gamma \frac{a_0'}{a_0} \tag{34}$$

In (27) - (34) we need several a_i' and c_i'. We get these from the defining equations $Q(a_i)$ and $R(c_1, c_2)$.

Derivative of a_0. By $Q(a_i) = k\gamma\lambda_i/\omega_i$ we have

$$\frac{a_0 q'(a_0)}{q(a_0)} = \frac{k\gamma\lambda_0}{\omega_0} \quad \Leftrightarrow \quad \frac{a_0}{k\gamma\lambda_0} = \frac{q(a_0)}{\omega_0 q'(a_0)}$$

Taking the derivative of both sides wrt. ω_i yields

$$\begin{aligned} \frac{a_0'}{k\gamma\lambda_0} &= \frac{a_0' q'(a_0) \omega_0 q'(a_0) - q(a_0) \left(-q'(a_0) + \omega_0 a_0' q''(a_0) \right)}{\omega_0^2 q'(a_0)^2} \\ &= \frac{a_0'}{\omega_0} + \frac{q(a_0)}{\omega_0^2 q'(a_0)} - \frac{a_0' q''(a_0) q(a_0)}{\omega_0 q'(a_0)^2} \\ \Longleftrightarrow \frac{a_0' q'(a_0)}{q(a_0)} &= \frac{1}{\omega_0 \left(\frac{\omega_0}{k\gamma\lambda_0} + \frac{q''(a_0) q(a_0)}{q'(a_0)^2} - 1 \right)} \end{aligned}$$

The last step is obtained by collecting all terms with a_0' on the left, multiplying with $q'(a_0)/q(a_0)$ and dividing through the term in brackets. We define

$$C(x) := \left(\frac{q(x)}{xq'(x)} + \frac{q''(x)q(x)}{q'(x)^2} - 1 \right).$$

Using $Q(a_i) = k\gamma\lambda_i/\omega_i$ the preceding equation becomes

$$\frac{a'_{0,\omega_1} q'(a_0)}{q(a_0)} = \frac{a'_{0,\omega_2} q'(a_0)}{q(a_0)} = \frac{1}{\omega_0 \left(\frac{q(a_0)}{a_0 q'(a_0)} + \frac{q''(a_0)q(a_0)}{q'(a_0)^2} - 1 \right)} = \frac{1}{\omega_0 C(a_0)}.$$

We use equation $Q(a_i) = k\gamma\lambda_i/\omega_i$ again to get

$$k\gamma \frac{a'_{0\omega_1}}{a_0} = k\gamma \frac{a'_{0\omega_2}}{a_0} = \frac{1}{\lambda_0 \left(\frac{q(a_0)}{a_0 q'(a_0)} + \frac{q''(a_0)q(a_0)}{q'(a_0)^2} - 1 \right)} = \frac{1}{\lambda_0 C(a_0)}$$

Derivative of a_1. As for a_0 we get

$$k\gamma \frac{a'_{1\omega_1}}{a_1} = -\frac{1}{\lambda_1 \left(\frac{q(a_1)}{a_1 q'(a_1)} + \frac{q''(a_1)q(a_1)}{q'(a_1)^2} - 1 \right)} = -\frac{1}{\lambda_1 C(a_1)}$$

$$\frac{a'_{1\omega_1} q'(a_1)}{q(a_1)} = -\frac{1}{\omega_1 \left(\frac{q(a_1)}{a_1 q'(a_1)} + \frac{q''(a_1)q(a_1)}{q'(a_1)^2} - 1 \right)} = -\frac{1}{\omega_1 C(a_1)}.$$

The remaining a_i-derivatives can be calculated in a similar way. For $\omega_i = \lambda_i = \frac{1}{3}$ (then $a_i = s, c_i = 1$) we get

$$k\gamma \frac{a_i'}{a_i} \quad \text{and} \quad \frac{a_i' q'(a_i)}{q(a_i)} \quad \text{is} \quad \frac{3}{C(s)} \text{ for } i = 0 \text{ and } -\frac{3}{C(s)} \text{ for } i = 1, 2. \tag{35}$$

Derivatives of c_i By $R(c_1, c_2) = (k\lambda_1, k\lambda_2)$ we have

$$\frac{c_1 r_{c_1}(1, c_1, c_2)}{r(1, c_1, c_2)} = k\lambda_1 \quad \Longleftrightarrow \quad \frac{c_1}{k} = \frac{\lambda_1 r(1, c_1, c_2)}{r_{c_1}(1, c_1, c_2)}$$

Taking the derivative wrt. λ_1 leads to (omitting the argument 1)

$$c'_{1\lambda_1} \left(\frac{1}{k} - \lambda_1 + \lambda_1 \frac{r(c_1, c_2) r_{c_1,c_1}(c_1, c_2)}{r_{c_1}(c_1, c_2)^2} \right) =$$
$$= \lambda_1 c'_{2\lambda_1} \left(\frac{r_{c_2}(c_1, c_2)}{r_{c_1}(c_1, c_2)} - \frac{r(c_1, c_2) r_{c_1,c_2}(c_1, c_2)}{r_{c_1}(c_1, c_2)^2} \right) + \frac{r(c_1, c_2)}{r_{c_1}(c_1, c_2)} \tag{36}$$

Also by $R(c_1, c_2) = (k\lambda_1, k\lambda_2)$ we have

$$\frac{c_2 r_{c_2}(c_1, c_2)}{r(c_1, c_2)} = k\lambda_2 \quad \Longleftrightarrow \quad \frac{c_2}{k\lambda_2} = \frac{r(c_1, c_2)}{r_{c_1}}$$

Taking the derivative wrt. λ_1 again leads to

$$\begin{aligned} c'_{2\lambda_1}\left(\frac{1}{k\lambda_2} - 1 + \frac{r(c_1, c_2) r_{c_2,c_2}(c_1, c_2)}{r_{c_2}(c_1, c_2)^2}\right) = \\ = \lambda_1 c'_{1\lambda_1}\left(\frac{r_{c_1}(c_1, c_2)}{r_{c_2}(c_1, c_2)} - \frac{r(c_1, c_2) r_{c_2,c_1}(c_1, c_2)}{r_{c_2}(c_1, c_2)^2}\right) \end{aligned} \tag{37}$$

Again we consider the point $\lambda_1 = \lambda_2 = \frac{1}{3}$ then $c_1 = c_2 = 1$ and equations (36) and (37) yield

$$2c'_{1\lambda_1} = c'_{2\lambda_1} + 9 \quad \text{and} \quad 2c'_{2\lambda_1} = c'_{1\lambda_1}.$$

Therefore we have $\frac{c'_{1\lambda_1}}{c_1} = 6$ and $\frac{c'_{2\lambda_1}}{c_2} = 3$. Analogously for the derivatives wrt. λ_2 we get $\frac{c'_{1\lambda_2}}{c_1} = 3$ and $\frac{c'_{2\lambda_2}}{c_2} = 6$.

Putting the derivatives together we get from (27) - (34) the following Hessian-Matrix of $\ln \Psi(\bar{\omega}, \bar{\lambda})$ at the point $\omega_i = \lambda_i = 1/3$, abbreviating $D = 3/C(s)$,

$$H = \begin{pmatrix} -2(\frac{1}{3} + D) & -(\frac{1}{3} + D) & 2D & D \\ -(\frac{1}{3} + D) & -2(\frac{1}{3} + D) & D & 2D \\ 2D & D & -2(\frac{8}{3}k\gamma + D) & -(\frac{8}{3}k\gamma + D) \\ D & 2D & -(\frac{8}{3}k\gamma + D) & -2(\frac{8}{3}k\gamma + D) \end{pmatrix}$$

H is negative definite iff $-H$ is positive definite.

Lemma 21 (Jacobi) *A matrix $A = A^T = (a_{ij}) \in \mathbb{R}^{n \times n}$ is positive definite iff the determinants of ist n main-sub-matrices S_i are positive.*

$$S_1 = a_{11}, \quad S_2 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \ldots, \quad S_k = \begin{pmatrix} a_{11} & \ldots & a_{1k} \\ \vdots & & \vdots \\ a_{k1} & \ldots & a_{kk} \end{pmatrix}, \ldots, \quad S_n = A$$

By Lemma 21 $-H$ is positive definite, as $D > 0$ as $C(x) > 0$ for $x > 0$, and

$$\det S_1 = 2\left(\frac{1}{3} + D\right) > 0$$

$$\det S_2 = 3\left(\frac{1}{3} + 2D + 3D^2\right) > 0$$

$$\det S_3 = \frac{16}{9}k\gamma + \frac{2}{3}D + \frac{32}{3}k\gamma D + 2D^2 + 16k\gamma D^2 > 0$$

$$\det S_4 = \det(-H) = \frac{64}{9}k^2\gamma^2 + D^2 + 64k^2\gamma^2 D^2 + 16k\gamma D^2 + \\ + \frac{128}{3}k^2\gamma^2 D + \frac{16}{3}k\gamma D > 0.$$

Theorem 15 (repeated) Let $U = \mathcal{U}_\varepsilon(1/3, 1/3)$. There is an $\varepsilon > 0$ such that $\sum_{\bar\lambda,\bar\omega\in U} N(\bar w, \bar l)/N_0 \; < \; C \cdot 3^{(1-\gamma)n}$.

Proof. For $\bar\lambda, \bar\omega \in U$ and a_i given by $Q(a_i) = \lambda_i k\gamma/\omega_i$ and $c_0 = 1$ and $R(c_1, c_2) = (\lambda_1 k,\ \lambda_2 k)$ we have $\frac{N(\bar w,\bar l)}{N_0} \; \le \; O\left(\frac{1}{n^2}\right) \varPsi(\bar\omega\,,\ \bar\lambda\,,\ \bar a\,,\ \bar c\,)^n$ by Corollary 12. Let $\bar x = (x_1, \ldots, x_4)$ and $h(\bar x) = \ln \varPsi(\bar\omega\,,\ \bar\lambda\,,\ \bar a\,,\ \bar c\,)$ with $\omega_1 = x_1, \omega_2 = x_2, \lambda_1 = x_3, \lambda_2 = x_4$ and a_i, c_i as before for $\bar\omega, \bar\lambda \in U$. Let $\overline{1/3} = (1/3, 1/3, 1/3, 1/3)$ then $h(\overline{1/3}) = \ln 3^{1-\gamma}$, $h_{x_i}(\overline{1/3}) = 0$ and $-\text{Hess}(h)(\overline{1/3})$, $\text{Hess}(h)$ the Hessian matrix of h, is positive definite (proved above, note $\text{Hess}(h)(\overline{1/3}) = H$.) We abbreviate $h_{i,j} = h_{x_i,x_j}(\overline{1/3})$ and by Taylor's Theorem we have for $\sum_i x_i^2 \; \to \; 0$

$$h(\overline{1/3} + \bar x) \; = \; h(\overline{1/3}) \; - \; \frac{1}{2} \; \sum_i \sum_j -h_{i,j}x_i x_j \; + \; o(\sum_i x_i^2)$$

$$\le \; h(\overline{1/3}) \; - \; \frac{1}{2} \; \left(\sum_i -(h_{i,i} + \delta)x_i^2 \; + \; \sum_i \sum_{j\neq i} -h_{i,j}x_i x_j \right) \tag{38}$$

with δ arbitrarily small for $\sum_i x_i^2$ small enough. We pick δ such that $-(\text{Hess}(h)(\overline{1/3}) + \delta I)$ is still positive definite.

We consider (38) with $x_1 = w_1/n - 1/3,\;\; x_2 = w_2/n - 1/3$ and $x_3 = l_1/(k\gamma n) - 1/3 \;\; x_4 = l_2/(k\gamma n) - 1/3$. Then

$$\sum_{\bar\omega,\bar\lambda\in U} \varPsi(\bar\omega\,,\ \bar\lambda\,,\ \bar a\,,\ \bar c\,)^n \; = \; \sum_{\bar\omega,\bar\lambda\in U} \exp(h(x_1, x_2, x_3, x_4)n)$$

$$\le \; 3^{(1-\gamma)n} \cdot \sum_{\bar\omega,\bar\lambda\in U} \exp\left[-\frac{1}{2} \left(\sum_i -(h_{i,i} + \delta)x_i^2 \; + \; \sum_i \sum_{j\neq i} -h_{i,j}x_i x_j \right) n \right] \tag{39}$$

Note that $\omega_i = w_i/n$, $\lambda_i = l_i/(k\gamma n)$, w_i, l_i integer. We distribute the factor n into the x_i multiplying each x_i with $\sqrt{n}$: $x_1\sqrt{n} = w_1/\sqrt{n} - \sqrt{n}/3$ and $x_3\sqrt{n} = l_1/(k\gamma\sqrt{n}) - \sqrt{n}/3$. As w_i, l_i are integers, the sum in (39) multiplied with $1/(\sqrt{n}^4(k\gamma)^2)$ is a Riemannian sum of the integral $\int\int\int\int \exp[-(1/2)(-(h_{i,i}+\delta)x_i^2 + \sum_i \sum_{j\neq i} -h_{i,j}x_ix_j)]dx_1dx_2dx_3dx_4$ with bounds $-\infty$, ∞ for each x_i. Following [22], page 71, the integral evaluates to $(2\pi)^2/\sqrt{D}$ where $D > 0$ is the determinant of $(-h_{i,j}) + \delta I$. Thus for n large the sum in (39)is $(2\pi)^2/\sqrt{D}(1+o(1))\sqrt{n}^4(k\gamma)^2 = O(n^2)$. The claim follows.

5 Remaining proofs

5.1 Local limit consideration

Lemma 6 (repeated) Let $Cn \geq m \geq (2+\varepsilon)n,\ C, \varepsilon > 0$ constants. Then

$$M(m,n) = \Theta(1)\cdot\left(\frac{m}{ae}\right)^m \cdot q(a)^n \text{ with } a \text{ defined by } Q(a) = \frac{m}{n}$$

Proof. As $Q(x)$ is increasing the assumptions for m/n imply that a is bounded away from 0 and ∞. Let $X = X(x)$ be a random variable with Prob$[X = j] = (x^j/j!)/q(x),$ for $j \geq 2$, and let $X_1, \ldots, X_n$ be independent copies of X. Then

$$\sum_{l_i\geq 2}\binom{m}{l_1,\ldots,l_n} = \text{Prob}[X_1+\cdots+X_n = m]\cdot\frac{q(x)^n}{x^m}\cdot m!.$$

We have E$[X] = xq'(x)/q(x) = Q(x)$. We pick $x = a$ then E$[X] = m/n$, E$[X_1+\cdots+X_n] = m$. The bounds on a imply that $C >$ VAR$[X] > \varepsilon > 0$ (constants ε, C not the same as above.) Therefore the Local Limit Theorem for lattice type random variables , cf. [4] , Theorem 5. 2, page 112, implies that Prob$[X_1+\cdots+X_n = m] = \Theta\left(\frac{1}{\sqrt{m}}\right)$. Applying Stirling's formula in the form $m! = \Theta(\sqrt{m})\left(\frac{m}{e}\right)^m$ yields the claim.

We come to Lemma 11. First we show that $R(c_1,c_2) = (R_1(c_1,c_2), R_2(c_1,c_2)) = (k\lambda_1, k\lambda_2)$ with $R_i(x_1,x_2) = \frac{x_ir_{x_i}(1,x_1,x_2)}{r(1,x_2,x_2)}$ defines $c_i = c_i(\lambda_1,\lambda_2)$ and that c_i is differentiable with respect to λ_i for $(\lambda_1,\lambda_2) \in \mathcal{U}_\varepsilon(1/3,1/3)$. By the theory of implicit function of several variables we need to show that the Jacobian Determinant of $R(x_1,x_2)$ is $\neq 0$ for $x_1 = x_2 = 1$. The Jacobian Matrix of $R(x_1,x_2)$ is , omitting the arguments x_i, recalling that $r = r(1,x_1,x_2)$ is our polynomial,

$$J = \frac{1}{r^2}\begin{pmatrix} (r_{x_1} + x_1r_{x_1,x_1})r - x_1r_{x_1}^2 & x_1r_{x_1,x_2}r - x_1r_{x_1}r_{x_2} \\ \\ x_2r_{x_1,x_2}r - x_2r_{x_1}r_{x_2} & (r_{x_2} + x_2r_{x_2,x_2})r - x_2r_{x_2}^2 \end{pmatrix}.$$

For $x_1 = x_2 = 1$ we get the following values: $r = r(1,1,1) = 3^{k-1}$, $r_{x_1} = r_{x_2} = k3^{k-2}$, $r_{x_1,x_1} = r_{x_2,x_2} = r_{x_1,x_2} = k(k-1)3^{k-3}$. ¿From this we get that the determinant of J for $x_1 = x_2 = 1$ is .... $\neq 0$.

Lemma 11 (repeated) There is an $\varepsilon > 0$ such that for $(\lambda_1, \lambda_2) \in \mathcal{U}_\varepsilon(1/3, 1/3)$

$$K(\bar{l}) = O\left(\frac{1}{n}\right) \cdot \frac{r(1, c_1, c_2)}{c_1^{l_1} c_2^{l_2}} \text{ with } R(c_1, c_2) = (k\lambda_1, k\lambda_2) \text{ defining } c_1, c_2.$$

Proof. The previous consideration shows that (c_1, c_2) is close to $(1,1)$ and well-defined. Let $(X, Y) = (X(x_1, x_2), Y(x_1, x_2))$ be the random vector with

$$\text{Prob}[(X,Y) = (k_1, k_2)] = \frac{\binom{k}{k-k_1-k_2,\, k_1,\, k_2} x_1^{k_1} x_2^{k_2}}{r(1, x_1, x_2)} \text{ if } k_1 = k_2 \mod 3$$

and 0 otherwise. Then $E(X, Y) = (R_1(x_1, x_2),\ R_2(x_1, x_2))$. We consider m independent copies $(X_i\, , Y_i)$ of $(X,\ Y)$ with $(x_1,\ x_2) = (c_1,\ c_2)$. Then $E\left[\sum_i (X_i, Y_i)\right] = (k\lambda_1 m,\ k\lambda_2 m) = (l_1, l_2)$. Let DCo be the determinant of the covariance matrix of (X, Y). We show below that for (c_1, c_2) close to $(1,1)$ we have that $DCo > 0$ for constants. The Local Limit Theorem for lattice random vectors [23], Theorem 22.1, Corollary 22.2 with $k = 2$ shows that Prob$[\sum_i (X_i, Y_i) = (k\lambda_1 m,\ k\lambda_2 m)] = \Theta(1/m)$. This implies the claim.

The covariance matrix of (X, Y) is defined as

$$Co = \begin{pmatrix} EX^2 - (EX)^2 & E[XY] - E[X]E[Y] \\ E[XY] - E[X]E[Y] & EY^2 - (EY)^2 \end{pmatrix}.$$

For $(X, Y) = (X(x_1, x_2), Y(x_1, x_2))$ we get

$$EX^2 = \frac{x_1(x_1 r_{x_1,x_1}(1, x_1, x_2) + r_{x_1}(1, x_1, x_2)}{r(1, x_1, x_2))},$$

$$EY^2 = \frac{x_2(x_2 r_{x_2,x_2}(1, x_1, x_2) + r_{x_2}(1, x_1, x_2)}{r(1, x_1, x_2))},$$

$$E[XY] = \frac{x_1 x_2 r_{x_1 x_2}(1, x_1, x_2)}{r(1, x_1, x_2)}.$$

This leads to a matrix similar to the Jacobian Matrix above: For $x_1 = x_2 = 1$ its determinant is positive.

5.2 The sharp threshold

To prove the sharp threshold we apply a general theorem. Let $A \subseteq \{0,\,1\}^N$ and let a_m be the number of elements of A with exactly m $1'$s. We let $\mu_p(A) \;=\; \sum_{m=0}^N\, a_m \cdot p^m \cdot (1 - p)^{N-m}$ be the probability of A, note $a_m \leq \binom{N}{m}$. If A is a non-trivial, monotone set we have that $\mu_p(A)$ is a strictly increasing, continuous, differentiable function in $0 \leq p \leq 1$. In this case for $0 \leq \tau \leq 1$ we have that p_τ is well defined by $\mu_{p_\tau}(A) = \tau$. Not let $A = (A_n)_{n\geq 1}$ and let be A_n be monotone. We say that A has a coarse threshold iff there exist constants $0 < \rho < \tau < 1$ such that $(p_\tau - p_\rho)/p_\rho \;\geq \varepsilon$ for a constant ε (and infinitely many n.) We can assume that $p_\tau \;=\; O(p_\rho)$ otherwise the threshold is clearly coarse. Moreover, we assume that $p_{1-o(1)} \;=\; o(1)$.

Theorem 22 (Bourgain, [13] , Theorem 2.2) *There exist functions $\delta \;=\; \delta(C, \tau) \;>\; 0$ and $K \;=\; K(C, \tau)$ such that the following holds: Let $A \;=\; A_n$ with $A \;\subseteq\; \{0,\,1\}^N$ be a monotone set with $\tau \;\leq\; \mu_p(A) \;\leq\; 1 - \tau$ for constant $1/2 \;>\; \tau \;>\; 0$ and assume that $p \cdot \frac{d\mu_p(A)}{dp} < C$. Then at least one of the following two possibilities holds:*
1.

$$\textit{Prob}_p[a \in A\;;\;\exists b \in A\;, |b| \leq K\;, b \subseteq a] \;>\; \delta$$

2. There exists $b\;\in \{0, 1\}^N$, $b \notin\; A\,, |b| \leq K$ such that the conditional probability

$$\textit{Prob}_p[a \in A\,|\,b \subseteq a] \;>\; \textit{Prob}_p[A] \;+\; \delta.$$

Corollary 23 *$A = (A_n)$ has a sharp threshold if $p_{1-o(1)} \;=\; O(p_\tau)$ for all $\tau > 0$, and for each $1/2 \;>\; \tau \;>\; 0,\, \delta \;>\; 0, \varepsilon \;>\; 0, K,\, p_\tau \;<\; p \;<\; p_{1-\tau}$ and all sufficiently large n the following two statements hold:*
1.

$$\textit{Prob}_p[a \in A\;;\;\exists b \in A\;, |b| \leq K\;, b \subseteq a] \;<\; \delta.$$

2. If $b\;\in\; \{0, 1\}^N$, $b \notin\; A\,, |b| \;\leq\; K$ with the conditional probability $\textit{Prob}_p[a \;\in\; A\,|\,b \subseteq a] \;>\; \textit{Prob}_p[A] \;+\; \delta$ then $\textit{Prob}_{p(1+\varepsilon)}[A] \;>\; 1 - \tau$

Proof. Assume, that A has a coarse threshold. Let $1 \;>\; \alpha \;>\; \beta \;>\; 0$ be such that $(p_\alpha - p_\beta)/p_\beta \;\geq\; \varepsilon$. We abbreviate $q \;=\; (p_\alpha + p_\beta)/2$. By strict monotonicity of $\mu_p(A)$ we have $\mu_q(A) \;=\; \gamma$ for a $\alpha \;>\; \gamma \;>\; \beta$. We have that $\frac{\gamma - \beta}{q - p_\beta} \;=\; \frac{d\mu_p(A)}{dp}|p \;=\; p^*$ for a $p_\beta \;<\; p^* \;<\; q$ (by the Mean Value Theorem.) We have that $(q - p_\beta)/p^* \;\geq\; \varepsilon'$ as $p^* \;=\; O(p_\beta)$. Therefore $\frac{\gamma-\beta}{q-p_\beta} \cdot p^* \;=\; \left(\frac{d\mu_p(A)}{dp}|p = p^*\right) \cdot p^* \leq C$ for a constant C. The preceding theorem applies to p^*. Our assumption implies that the first item of the theorem does not hold.

Therefore the second item of the preceding theorem must hold for $p = p^*$. We have that $p^* + \frac{p_\alpha - p_\beta}{2} < p_\alpha$. Therefore $p^* \left(1 + \frac{p_\alpha - p_\beta}{p^* \cdot 2}\right) < p_\alpha$. Moreover $\frac{p_\alpha - p_\beta}{p^* \cdot 2} > \varepsilon''$ as $p^* = O(p_\beta)$. Our second assumption shows that the preceding statement cannot hold. Therefore the second item of the preceding theorem does not hold, too. Therefore A cannot have a coarse threshold.

Let $F(n, p)$ be the random formula of equations $y_1 + \cdots + y_k = a \mod 3, 0 \leq a \leq 2$ over n variables where each equation is picked with probability c/n^{k-1} independently.

Lemma 24 *Unsatisfiability of $F(n, p)$ has a sharp threshold.*

Proof. We apply Corollary 23. Let $p = c/n^{k-1}$. Observe that $F(n, p)$ is unsatisfiable whp. for $c > 1$ by expectation calculation. Concerning the first item of the corollary we show that $F(n, p)$ does not contain a subformula over a bounded number of variables such that each variable occurs at least twice. The expected number of such subformulas over $1 \leq l \leq B$, B constant variables is bounded above by $\binom{n}{l} \cdot \left(c/n^{k-1}\right)^{2l/k} \leq O(1) \cdot n^{(2/k-1)l}$. As $k \geq 3$ and $l \geq 1$ the geometric series shows that the expectation of the number of such subformulas with $\leq B$ variables is $o(1)$. As each unsatisfiable formula contains a subformula where each variable occurs at least twice we have no unsatisfiable subformula of bounded size whp. The first item of the corollary holds.

Concerning the second item, let B be a fixed satisfiable formula and let $p < 1/n^{k-1}$. We assume that Prob[UNSAT$(B \cup F(n, p))$] $>$ Prob[UNSAT$(F(n, p))$] $+ \delta$. UNSAT(F) is the event that F is unsatisfiable. With high probability $F(n, p)$ contains only equations with 1 or none variables from B (as $p < 1/n^{k-1}$ and the number of variables of B is constant.)

Consider a fixed satisfiable formula F over the variables not in B We pick each equation with exactly one variable in B with probability $p = c/n^{k-1}$ independently. We assume that the resulting random formula is unsatisfiable with probability $\delta > 0$. We show that this implies that the random instance obtained from F by adding *each* equation with probability ε/n^{k-1}, independently, $\varepsilon > 0$ constant. is unsatisfiable with high probability. This directly implies that the second item of Corollary 23 holds.

Consider a fixed variable x of F. We throw in the equations containing x with ε/n^{k-1}, We show below that the resulting random formula is unsatisfiable with probability $\delta' > 0$, δ' constant. Throwing *each* equation with probability ε/n^{k-1}, the expected number of variables x such that the equations containing x lead to unsatisfiability of F is $\delta' n$. For $x \neq x'$ the equations with x or x' are nearly independent. Tschebycheff's inequality shows that we even have a linear number of variables x whose equations yield unsatisfiability whp.

We show the statement above concerning the fixed variable x. When throwing in the equations with one variable in B with $p = c/n^{k-1}$ we get with probability δ a set U such that $F \cup B \cup U$ is unsatisfiable. With probability slightly lower, but still constant > 0 we can assume that U is of bounded size. Now consider a satisfying assignment a of B. We replace the variable from B in each equation by its value under a and get a set of equations with $k - 1$ variables each. When we add these equations to F the resulting formula is unsatisfiable.

Now consider our variable x from F and throw in each equation containing x with probability ε/n^{k-1}. With constant probability > 0 we get the a set U' obtained from a set U as above by replacing the variable from B by x. With the same probability we get U_0 instead of U' where U_0 is obtained as follows: Let E be an equation of U such that the variable from B has the value j in the satisfying assignment a from B. The variable from B is replaced with x in E and we subtract j from the right hand side. The resulting formula is unsatisfiable for all assignments which have $x = 0$. U_1 is defined by adding $1 - j$ to the right hand-side. The resulting formula is unsatisfiable for $x = 1$. U_2 is defined by adding $2 - j$ and the resulting formula is unsatisfiable for $x = 2$. With constant probability > 0 we get one such set U_j.

To get unsatisfiability for all 3 values of x we observe that with probability roughly δ^3 we get three sets U, V, W with one variable in B which are disjoint and each of them causes unsatisfiability. This implies that with constant probability > 0 we get three sets U_0, V_1, W_2 of equations with x. The resulting formula is unsatisfiable for any value of x.

II. Uniquely extendible constraints

1 Outline

A uniquely extendible constraint C on a given domain D is a function from D^k to true, false with the following restriction: For any argument list with a gap at an arbitrary position, like $(d_1, \ldots d_{i-1}, -, d_{i+1}, \ldots, d_k)$ there is a unique $d \in D$ such that $C(d_1, \ldots d, \ldots, d_k)$ evaluates to true. Note that $C(d_1, \ldots, d, \ldots, d_k) =$ true implies that $C(d_1, \ldots, d', \ldots, d_k) =$ false for $d \neq d'$. The random constraint is a uniform random member from the set of all uniquely extendible constraints over D. Let $\mathit{\Gamma}$ be the set of all such constraints. Typical examples of such constraints are linear equations with k variables, modulo $|D|$. A threshold result analogous to Lemma 24 can be proved by similar arguments based on symmetry properties of uniquely extendible constraints.

Given a set of n variables a clause is an ordered k-tuple of variables equipped with a uniquely extendible constraint. The number of all formulas with m clauses is $M(km, n) \cdot |\mathit{\Gamma}|^m$, we denote $N_0 = M(km, n)$ (notation cf. (1).) A random formula is a uniform random element of the set of all formulas. The random variable X gives the number of solutions of a formula and $\mathrm{E}[X] = (1/d)^{(1-\gamma)n}, m = \gamma n$. This follows from symmetry considerations. For two assignments a, b we study $\mathrm{E}[X_a X_b]$ where X_a is $= 1$ iff the formula is true under a. It turns out that $\mathrm{E}[X_a X_b]$ depends only on the number of variables which have different values under a, b. Let DIFF$(a, b) =$ the set of variables with different values under a and b.

Given a k-tuple a of values from D and another k-tuple b differing from a in exactly $i,\ 0 \leq i \leq k$, slots, we let p_i be the probability that the random constraint is true under b conditional on the event that it is true under a. The following very simple generating polynomial for the $\binom{k}{i} \cdot p_i$ is the observation making our proof possible.

Lemma 25 *(a) (From [6])* $p_0 = 1,\ p_{i+1} = \frac{1}{d-1}(1 - p_i)$.
(b)

$$\textit{Let } p(z) = \frac{1}{d}\left((1+z)^k + (d-1)\left(1 - \frac{z}{d-1}\right)^k\right) \textit{ then } p(z) = \sum_i \binom{k}{i} p_i \cdot z^i$$

Proof. (b) We need to show that $p_i = \frac{1}{d}\left(1 + (-1)^i \left(\frac{1}{d-1}\right)^{i-1}\right)$. This holds for $i = 0, i = 1$. For $i > 1$ we get by induction:

$$p_i = \frac{1}{d-1}(1 - p_{i-1}) = \frac{1}{d-1}\left(1 - \frac{1}{d}\left(1 + (-1)^{i-1}\left(\frac{1}{d-1}\right)^{i-2}\right)\right) =$$

$$= \frac{1}{d-1} - \frac{1}{d(d-1)} - \frac{1}{d}(-1)^{i-1}\left(\frac{1}{d-1}\right)^{i-1} = \frac{1}{d}\left(1 + (-1)^i\left(\frac{1}{d-1}\right)^{i-1}\right).$$

We let $C_j = \frac{|\Gamma|}{d} \cdot \binom{k}{j} \cdot p_j$ for $0 \le j \le k$, $K(l) = \sum_{j_1+\cdots+j_m=l} C_{j_1} \cdots C_{j_m}$.

Then $\hat{N}(w, l) = M(l, w)M(km - l, n - w)K(l)$

is the number of formulas F true under two assignments a, b with $|\text{DIFF}(a, b)| = w$ and the variables with different values occupy exactly l slots of F. The factors $\binom{k}{j}$ of C_j count how to distribute the l slots. The factor $M(l, w)M(km - l, n - w)$ counts how to place the variables into these slots. The factors $\frac{|\Gamma|}{d} \cdot p_j$ count the number of constraints such that the formula becomes true under a, b. Given an assignment a the number of assignment formula pairs (b, F) with $|\text{DIFF}(a, b)| = w$, F is true under a, b, and the variables from $\text{DIFF}(a, b)$ occupy exactly l slots is

$$N(w, l) = \binom{n}{w}(d-1)^w \cdot \hat{N}(w, l). \text{ And } \mathrm{E}[X^2] = d^n \sum_{w,l} N(w, l) \cdot \frac{1}{N_0 \cdot |\Gamma|^m}$$

The next theorem is analogous to Theorem 5.

Theorem 26 $\sum_{w,l} N(w, l)/(N_0|\Gamma|^m) \le C d^{(1-2\gamma)n}$, $k \ge 8$, $m = (1-\gamma)n$.

We let $\lambda = l/km$ and $\omega = w/n$ with w, l always having the meaning above. The proof of Theorem 26 follows the pattern of Theorem 5. We omit all steps referring to the summation, they are quite analogous. The details to bound the summands are however different. We have

$$K(l) = \text{Coeff}[z^l, p(z)^m] \cdot \left(\frac{|\Gamma|}{d}\right)^m \le \left(\frac{p(c)|\Gamma|}{d}\right)^m \cdot \frac{1}{c^l} \text{ for } c > 0.$$

We define $\Psi(\omega, \lambda, x, y, z) :=$

$$\left(\frac{(d-1)q(x)}{q(s)\omega}\right)^{\omega} \left(\frac{q(y)}{q(s)(1-\omega)}\right)^{1-\omega} \cdot \left(\frac{\lambda s}{xz}\right)^{\lambda k \gamma} \left(\frac{(1-\lambda)s}{y}\right)^{(1-\lambda)k\gamma} \cdot \left(\frac{p(z)}{d}\right)^{\gamma}.$$

We have $\Psi(1-1/d,\ 1-1/d,\ s,\ s,\ d-1)\ =\ d^{1-2\gamma}$, s is given by $Q(s)=k\gamma$, cf. discussion around Lemma 6. As Lemma 8 we have the next Lemma; the subsequent Theorem is as Theorem 9.

Lemma 27 $N(w,l)/(N_0|\Gamma|^m)\ \leq\ \Psi(\omega,\lambda,a,b,c)\cdot O(n)$ *for* $a,b,c>0$.

Observe that for $Q(s)=k\gamma\geq 8$ we have $s\geq 7$.

Theorem 28 *Let* $d=4$ *and* $s\geq 7$. *For any* $\lambda>0$ *there exist* $a,b,c>0$ *such that:*
(1) $\Psi(\omega,\lambda,a,b,c)\ \leq\ d^{1-2\gamma}$.
(2) For any $\varepsilon>0$, λ *not* $\varepsilon-$*close to* $1-1/d$, $\Psi(\omega,\lambda,a,b,c)\ \leq\ d^{1-2\gamma}-\delta$.

Two reals a,b are $\varepsilon-$close iff $|a-b|<\varepsilon$. To treat λ close to $(d-1)/d$ we consider the function $P(z)=zp'(z)/p(z)$ (cf. discussion after Corollary 10.) We have $P(d-1)=k(1-1/d)$ and the derivative $P'(d-1)>0$. Thus we can define $c=c(\lambda)$ for λ $\varepsilon-$close to $1-1/d$ by $P(c)=k\lambda$. And $c(\lambda)$ is differentiable. As Lemma 11, Corollary 12, and Lemma 13 we get the next 3 items. To prove Lemma 31 the Hessian matrix of $\Psi(\omega,\lambda,a,b,c)$ is considered (calculation analogously to [5].)

Lemma 29 *There is an* $\varepsilon>0$ *such that for* ω,λ $\varepsilon-$*close to* $1-1/d$ *we have* $K(l)=O(1/\sqrt{n})\cdot(p(c)|\Gamma|/d)^m\cdot 1/c^l$ *with* $P(c)=k\lambda$.

Corollary 30 *There is an* $\varepsilon>0$ *such that for* ω,λ *being* $\varepsilon-$*close to* $1-1/d$ $N(w,l)/(N_0|\Gamma|^m)\leq O(1/n)\cdot\Psi(\omega,\ \lambda,\ a,\ b,\ c)$ *with* $Q(a)=l/w, Q(b)=(km-l)/(n-w), P(c)=\lambda k$.

Lemma 31 *The function* $\Psi(\omega,\lambda,a,b,c)$ *with* a,b,c *given by* $Q(a)=l/w, Q(b)=(km-l)/(n-w), P(c)=\lambda k$ *has a local maximum with value* $d^{1-2\gamma}$ *for* $\lambda=\omega=1-1/d$. *In this case we have* $a=b=s$ *and* $c=d-1$.

$$\text{We define }\ \mathrm{OPT}_1(x,y,s)\ =\ (d-1)\cdot\frac{q(sx)}{q(s)}\ +\ \frac{q(sy)}{q(s)},$$

$$\mathrm{OPT}_2(x,y,z,s)\ =\ \left(\frac{1}{y+xz}\right)^Q,\ y+xz>0$$

$$\mathrm{OPT}_3(z,s)\ =\ (1+z)^Q\ +\ (d-1)\cdot\left|1\ -\ \frac{z}{d-1}\right|^Q,\ Q=Q(s)$$

$$\mathrm{OPT}(x,y,z,s)\ =\ \mathrm{OPT}_1(x,y,s)\cdot\mathrm{OPT}_2(x,y,z,s)\cdot\mathrm{OPT}_3(z,s).$$

As Lemma 16 we have the next Lemma. We prove Theorem 28 based on this lemma. We cannot proceed analogously to the proof of Theorem 9 because the polynomial $p(z)$ is not as symmetric as $r(x_0,x_1,x_2)$. The two cases λ small (in Section 2) and λ large (in Section 3) are treated separately.

Lemma 32

Let $a, b, c > 0$ *be such that* $\dfrac{\lambda}{1-\lambda} = \dfrac{ac}{b}$. *Then* $\Psi(\omega, \lambda, as, bs, c) \le \dfrac{1}{d^{2\gamma}} OPT(a, b, c, s)$.

2 Proof of Theorem 28 for $d = 4,\ s \ge 7,\ \lambda \le 1 - 1/d$

We restrict attention to $d = 4$ fix $b = 1$ and consider c, a with $0 \le c \le 3$ and $0 \le a \le 1$. With these values $\mathrm{OPT}(a, b, c, s)$ leads to the following notation used in this Section.

$$\mathrm{OPT}_1(a, s) = 3 \cdot \frac{q(sa)}{q(s)} + 1 \ , \ \mathrm{OPT}_2(a, c, s) = \left(\frac{1}{1+ac}\right)^Q$$
$$\mathrm{OPT}_3(c, s) = (1+c)^Q + 3 \cdot \left(1 - \frac{c}{3}\right)^Q$$
$$\mathrm{OPT}(a, c, s) = \mathrm{OPT}_1(a, s) \cdot \mathrm{OPT}_2(a, c, s) \cdot \mathrm{OPT}_3(c, s).$$

The values of $\mathrm{OPT}(a, c, s)$ at the corners of the rectangle for $0 \le c \le 3,\ 0 \le a \le 1$ are:

$$\begin{aligned} \mathrm{OPT}(0, 0, s) &= 4 \quad , \ \mathrm{OPT}(0,\ 3,\ s) = 4^Q \\ \mathrm{OPT}(1, 0, s) &= 4^2 \quad , \ \mathrm{OPT}(1,\ 3,\ s) = 4 \end{aligned} \tag{40}$$

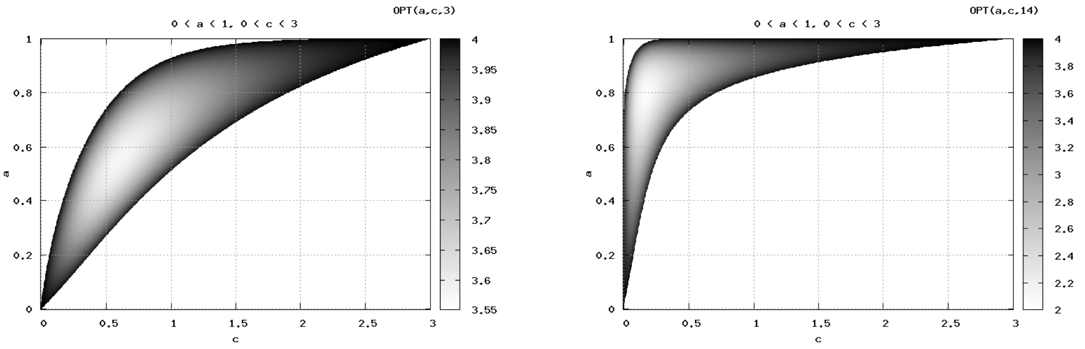


Fig. 2. $\mathrm{OPT}(a, c, s)$ over the rectangle $0 \le a \le 1, 0 \le c \le 3$ for $s = 3$ and $s = 14$.

We prove four lemmas. Observe that $A(c, s)$ in Lemma 33 is a flat linear function in $c \ge 0$ from $A(0, s) = 1 - \frac{7}{10Q}$ to $A(3, s) = 1$.

Lemma 33

$$\textit{Let } s \geq 7 \textit{ and let } A(c) = A(c,s) = \frac{7}{Q \cdot 10 \cdot 3} \cdot c + 1 - \frac{7}{10 \cdot Q}.$$
$$\textit{Then OPT}(A(c),\ c,\ s\,) \textit{ is strictly increasing in } 1 \leq c < 3.$$

$A(c,s)$ in the subsequent Lemma is a steep linear function starting at $A(0,s) = 0$.

Lemma 34

$$\textit{Let } s \geq 6 \textit{ and let } A(c) = A(c,s) = \frac{Q}{2} \cdot c\ .$$
$$\textit{Then OPT}(A(c),\ c,\ s) \textit{ is strictly decreasing for } 0 < c \leq \frac{1}{Q}$$

Lemma 35 *(a) For each constant $0 \leq a \leq 1$ OPT(a,c,s) as a function in c with $0 \leq c \leq 3$ has a unique local minimum.*
(b) For each constant $0 \leq c \leq 3$ OPT(a,c,s) as a function in a with $0 \leq a \leq 1$ has a unique local minimum.

Lemma 36 *Let $s \geq 6$ then OPT$(a,\ c,\ s\,) < 4 - \delta$ for $(a,\ c) =$*

$$= \left(\frac{1}{2}, \frac{1}{Q}\right), \left(\frac{1}{2}, \frac{2}{Q}\right), \left(\frac{2}{3}, \frac{2}{Q}\right), \left(\frac{2}{3}, \frac{3}{Q}\right), \left(1 - \frac{7}{15Q}, \frac{3}{Q}\right), \left(1 - \frac{7}{15Q}, 1\right)$$

Proof of Theorem 28 for $\lambda \leq 1 - 1/d$. (cf. proof of Theorem 9 after Lemma 20.) We have $\lambda \leq 1 - 1/d \iff \lambda/(1-\lambda) \leq d - 1$. Using Lemma 32 we need to show that for each $P \leq d - 1$ we have a decomposition $P = ac$ such that $\text{OPT}(a,c,s) \leq 4$ of $4 - \delta$. Lemma 33 treats $1 - 7/(15Q) \leq P \leq d - 1$. Lemma 36 together with Lemma 35 treat $1 - 7/(15Q) \geq P \geq 1/(2Q)$. Finally Lemma 34 treats $1/(2Q) \geq P > 0$. Observe that $\text{OPT}(0,0,s) = 4$ and we need to look into the proof of Lemma 32 to get the $-\delta$ required for small P. □

2.1 Proof of Lemma 33

Lemma 33 (repeated)

$$\textit{Let } s \geq 7 \textit{ and let } A(c) = A(c,s) = \frac{7}{Q \cdot 10 \cdot 3} \cdot c + 1 - \frac{7}{10 \cdot Q}.$$
$$\textit{Then OPT}(A(c),\ c,\ s\,) \textit{ is strictly increasing in } 1 \leq c < 3.$$

Proof.

$$\begin{aligned}
\text{Some notation:}\,\text{PPLUS3}(x,y) \;&=\; (1\,+\,x)^y \,+\, 3\left(1-\frac{x}{3}\right)^y,\; x\le 3 \\
\text{PMINUS}(x,y) \;&=\; (1\,+\,x)^y \,-\, \left(1-\frac{x}{3}\right)^y,\; x\le 3 \qquad (41)\\
\frac{d}{dc}\ln\text{PPLUS3}(c,Q) \;&=\; Q\cdot\frac{\text{PMINUS}(c,Q-1)}{\text{PPLUS3}(c,Q)}, \\
A \;=\; A(c),\; A' \;=\; \frac{d}{dc}A \;=\; \frac{7}{10\cdot 3\cdot Q}\;,\; & \frac{d}{dc}\ln\text{OPT}(A,c,s) \;=
\end{aligned}$$

$$= \frac{3\frac{\exp(As)-1)}{\exp(s)-s-1}\cdot sA'}{\text{OPT}_1(A,s)} - Q\cdot\frac{A'c\,+\,A}{1+Ac} + Q\cdot\frac{\text{PMINUS}(c,Q-1)}{\text{PPLUS3}(c,Q)} \;>=<0$$

$$\iff \frac{3\frac{\exp(As)-1}{\exp(s)-1}\cdot A'}{\text{OPT}_1(A,s)} - \frac{A+A'c}{1+Ac} + \frac{\text{PMINUS}(c,Q-1)}{\text{PPLUS3}(c,Q)} \;>=<\; 0 \qquad (42)$$

$$\text{(Division with } Q \;=\; \frac{s(\exp(s)-1)}{\exp(s)-s-1}\text{.)}$$

$$\text{For } c \;=\; 3 \text{ the derivative is } \;=0,\; A(3,s)=1 \text{ (OPT}(1,3,s)=4.)$$

We split the right-hand-side of (42) into two additive terms. Inequalities (43) and (44) imply that the $\frac{d}{dc}\,\text{OPT}(A,c,s) > 0$. For $c=3$ both left-hand-sides are $=0$.

$$\frac{3\frac{\exp(As)-1)}{\exp(s)-1}\cdot A'}{\text{OPT}_1(A,s)} - \frac{A'c}{1+Ac} \;>\; 0 \qquad (43)$$

$$-\frac{A}{1+Ac} + \frac{\text{PMINUS}(c,Q-1)}{\text{PPLUS3}(c,Q)} \;>\; 0 \qquad (44)$$

Proof of (43) for $0\le c<3$ and $s\ge 7$.

$$K \;:=\; \frac{\exp(sA)-1}{\exp(s)-1},\quad L := \frac{\exp(sA)-sA-1}{\exp(s)-s-1}$$

$$\text{We need to show } \frac{3KA'}{3L+1} \;>\; \frac{A'c}{1+Ac} \;\iff\; \frac{3K}{3L+1} \;>\; \frac{c}{1+Ac}$$

$$\iff\; 3\,(K+KAc-Lc) \;>\; c \quad \text{(For } c=3 \text{ both sides are } =3.) \qquad (45)$$

By (7) we have $L \;\le\; K$ and (45) is implied by

$$3K\,(1+Ac-c) \;>\; c \qquad \text{(For } c=3 \text{ both sides are } =3.) \qquad (46)$$

$K \geq 0$ is increasing and convex, $1 + Ac - c$ is > 0, and increasing for $c > 3/2$, and convex. Therefore the left-hand-side of (46) is convex for $c \geq 3/2$. Therefore, for $c \geq 3/2$, it follows from

$$\left(\frac{d}{dc}3K\left(1+Ac-c\right)\right)_{|c=3} < \left(\frac{d}{dc}c\right)_{|c=3} = 1. \tag{47}$$

$$\frac{d}{dc}3K\left(1+Ac-c\right) \quad = \frac{3\exp(sA)\cdot s\cdot\frac{7}{30Q}}{\exp(s)-1}\cdot\left(1+Ac-c\right) +$$

$$\frac{3(\exp(sA)-1)}{\exp(s)-1}\cdot\left(\frac{7}{30Q}c+\frac{7}{30Q}c+1-\frac{7}{10Q}-1\right).$$

$$\text{Therefore } \frac{d}{dc}3K\left(1+Ac-c\right)_{|c=3} =$$

$$\frac{7\exp(s)(\exp(s)-s-1)}{10(\exp(s)-1)^2} + \frac{21(\exp(s)-s-1)}{10s(\exp(s)-1)} \tag{48}$$

For $s = 7$ we get that (48) is < 0.995. Moreover it is decreasing in s (proof omitted) and (47) holds for all $s \geq 7$ and $c \geq 3/2$. For $c \leq 3/2$ we argue as in the proof of Lemma 20(a) cf. the argument following (20).

Proof of (44) for $1 \leq c < 3$ *and* $s \geq 5$ *.*

$$\text{We need to show } \frac{A}{1+Ac} < \frac{\text{PMINUS}(c,Q-1)}{\text{PPLUS3}(c,Q)}$$

$$\iff A \cdot \text{PPLUS3}(c,Q) < (1+Ac)\text{PMINUS}(c,Q-1)$$

$$\iff A\cdot(\text{PPLUS3}(c,Q) - c\cdot\text{PMINUS}(c,Q-1)) = A\cdot\text{PPLUS3}(c,Q-1)$$

$$< \text{PMINUS}(c,Q-1)$$

$$\iff A < \frac{\text{PMINUS}(c,Q-1)}{\text{PPLUS3}(c,Q-1)} = \frac{(1+c)^{Q-1}-(1-\frac{c}{3})^{Q-1}}{(1+c)^{Q-1}+3(1-\frac{c}{3})^{Q-1}} \tag{49}$$

(For $c = 3$ both sides of (49) are $= 1$.)

For $c = 1$ inequality (49) becomes

$$1-\frac{7}{15Q} < \frac{2^{Q-1}-\left(\frac{2}{3}\right)^{Q-1}}{2^{Q-1}+3\left(\frac{2}{3}\right)^{Q-1}} = 1-\frac{4\left(\frac{1}{3}\right)^{Q-1}}{1+3\left(\frac{1}{3}\right)^{Q-1}}$$

As $4\left(\frac{1}{3}\right)^{Q-1} < \frac{7}{15Q}$ for $Q \geq 5$, (49) holds for $c = 1$ and $s \geq 5$ as $Q \geq s$.

To show that (49) holds for all $3 \ > \ c \geq \ 1$ we show that the right-hand-side is concave for $c > 1$.

$$\text{Numerator of } \frac{d}{dc}\frac{\text{PMINUS}(c,Q-1)}{\text{PPLUS3}(c,Q-1)} \ =$$

$$(Q-1)\cdot\left((1+c)^{Q-2} \ + \ \frac{1}{3}\left(1-\frac{c}{3}\right)^{Q-2}\right)\cdot\left((1+c)^{Q-1} \ + \ 3\left(1-\frac{c}{3}\right)^{Q-1}\right) \ -$$

$$-\,(Q-1)\cdot\left((1+c)^{Q-1} \ - \ \left(1-\frac{c}{3}\right)^{Q-1}\right)\cdot\left((1+c)^{Q-2} \ - \ \left(1-\frac{c}{3}\right)^{Q-2}\right)$$

$$= \ (Q-1)\cdot(1+c)^{Q-2}\cdot\left(1-\frac{c}{3}\right)^{Q-2}\cdot\left(\left(\frac{1}{3}+1\right)(1+c) \ + \ \left(1-\frac{c}{3}\right)\cdot(1+3)\right)$$

$$= \ (Q-1)\cdot(1+c)^{Q-2}\cdot\left(1-\frac{c}{3}\right)^{Q-2}\cdot\left(\frac{1}{3}+3+2\right) \quad (50)$$

We have that $(1+c)\cdot\left(1-\dfrac{c}{3}\right)$ is decreasing for $c > 1,$ and PPLUS3$(c, Q-1)$ is increasing .

Therefore the right-hand-side of (49) is concave.

2.2 Proof of Lemma 34

Lemma 34 (repeated)

$$\text{Let } s \geq 6 \text{ and let } \; A(c) \;=\; A(c,s) \;=\; \frac{Q}{2} \cdot c\;.$$

$$\text{Then } \; \text{OPT}(A(c),\, c,\, s) \; \text{ is strictly decreasing for } 0 \; < c \; \leq \; \frac{1}{Q}$$

Proof. Analogously to (43) and (44) this follows from (51) and (52.) (Notation cf. (41.)

$$\text{with } A = A(c),\;\; A' \;=\; Q/2 \; \frac{3\frac{\exp(As)-1)}{\exp(s)-1}}{\text{OPT}_1(A,\; s)} A' \;-\; \frac{A'c}{1+Ac} \;<\; 0, \tag{51}$$

$$-\frac{A}{1+Ac} \;+\; \frac{\text{PMINUS}(c, Q-1)}{\text{PPLUS3}(c,Q)} \;<\; 0. \tag{52}$$

Proof of (51) for $s \geq 5.55$ *and* $0 \;<\; c \;\leq\; 1/Q$

$$K \;:=\; \frac{\exp(sA)-1}{\exp(s)-1},\;\; L := \frac{\exp(sA)-sA-1}{\exp(s)-s-1}$$

$$\text{We need to show } \frac{3KA'}{3L+1} \;<\; \frac{A'c}{1+Ac} \;\iff\; \frac{3K}{3L+1} \;<\; \frac{c}{1+Ac}$$

$$\iff\; 3\,(K+KAc-Lc) \;<\; c \text{ For } c=0 \text{ both sides are } \; = 0. \tag{53}$$

As $AK \;\leq\; L$ by (7) we get that (53) is implied by $3 \cdot K \;<\; c$. For $c \;=\; 0$ both sides of $3 \cdot K \;<\; c$ are 0. The left-hand-side is convex. It is sufficient to show $3 \cdot K \;<\; c.$ for $c = 1/Q$. Plugging in the definition of $1/Q$ for c and $A(1/Q\,, s) \;=\; 1/2$ into K we need to show

$$\frac{3\exp(s/2)-1}{\exp(s)-1} < \frac{\exp(s)-s-1}{s(\exp(s)-1)} \iff 3s\exp(s/2) \;<\; \exp(s)-1$$

For $s \geq 6$ the preceding inequality holds by simple consideration.

Proof of (52) for $s \geq 2$ *and* $c \leq 1/Q$ Analogously to the proof of (49) we need to show

$$A \;=\; \frac{Q}{2}c > \frac{\text{PMINUS}(c,Q-1)}{\text{PPLUS3}(c,Q-1)} \;=\; \frac{(1+c)^{Q-1}-(1-\frac{c}{3})^{Q-1}}{(1+c)^{Q-1}+3(1-\frac{c}{3})^{Q-1}} \tag{54}$$

$$\text{For } c = 0 \text{ both sides of the preceding inequality are } \; = 0$$

We show, that $A' >$ the derivative wrt. c of the right-hand-side of (54). Using (50) we need to show

$$\frac{Q}{2} \cdot \left((1+c)^{Q-1} + 3\left(1 - \frac{c}{3}\right)^{Q-1}\right)^2 \; > \; (Q-1) \cdot (1+c)^{Q-2} \cdot \left(1 - \frac{c}{3}\right)^{Q-2} \cdot \frac{16}{3}.$$

Note $Q \cdot (1+c)^{Q-1} \cdot \left(1 - \frac{c}{3}\right)^{Q-1} \cdot \frac{16}{3} \geq (Q-1) \cdot (1+c)^{Q-2} \cdot \left(1 - \frac{c}{3}\right)^{Q-2} \cdot \frac{16}{3}$

as $(1+c) \cdot \left(1 - \frac{c}{3}\right) \geq 1$ for $0 \leq c \leq 1/Q < 2$.

Enlarging the right-hand-side it is sufficient to show

$$3\left((1+c)^{Q-1} + 3\left(1 - \frac{c}{3}\right)^{Q-1}\right)^2 \; > \; (1+c)^{Q-1} \cdot \left(1 - \frac{c}{3}\right)^{Q-1} \cdot 32.$$

$$\Longleftrightarrow 3\left(1 + 3\left(\frac{1 - \frac{c}{3}}{1+c}\right)^{Q-1}\right)^2 \; > \; 32 \cdot \left(\frac{1 - \frac{c}{3}}{1+c}\right)^{Q-1}$$

Setting $x = \left(\frac{1-\frac{c}{3}}{1+c}\right)^{Q-1}$ it is easy to see that the preceding inequality holds for $x \geq 0$, and therefore clearly for $c \leq 1/Q < 3$.

2.3 Proof of Lemma 36 and Lemma 35

Lemma 35 follows by elementary consideration, see the analogous situation in the proof of Lemma 18(a) and Lemma 19 (a).

Lemma 36 **(repeated)** Let $s \geq 6$ then OPT$(a,\ c,\ s) < 4 - \delta$ for $(a,\ c) =$

$$= \left(\frac{1}{2},\ \frac{1}{Q}\right),\ \left(\frac{1}{2},\ \frac{2}{Q}\right),\ \left(\frac{2}{3},\ \frac{2}{Q}\right),\ \left(\frac{2}{3},\ \frac{3}{Q}\right),\ \left(1\ -\ \frac{7}{15Q},\ \frac{3}{Q}\right),\ \left(1\ -\ \frac{7}{15Q}\ ,\ 1\right)$$

Proof. The claim for $a = \frac{1}{2},\ c\ =\ \frac{1}{Q}$ is included in Lemma 34.

$$\text{FIRSUM}(a,c,s) \;=\; (1+c)^Q \text{OPT}_2(a,c,s) \;=\; \left(\frac{1+c}{1+ac}\right)^Q$$

$$\text{SECSUM}(a,c,s) \;=\; 3\left(1-\frac{c}{3}\right)^Q \text{OPT}_2(a,c,s) \;=\; 3\left(\frac{1-\frac{c}{3}}{1+ac}\right)^Q \text{ then}$$

$$\text{OPT}(a,c,s) \;=\; \text{OPT}_1(a,s)\cdot\left[\text{FIRSUM}(a,c,s) \;+\; \text{SECSUM}(a,c,s)\right].$$

$$\text{For } x,y \geq 0 \text{ we have FIRSUM}\left(x,\frac{y}{Q},s\right) \;=\; \left(\frac{1+\frac{y}{Q}}{1+x\cdot\frac{y}{Q}}\right)^Q \;=$$

$$= \left(1 \;+\; \frac{\frac{y}{Q}(1-x)}{1+x\frac{y}{Q}}\right)^Q \;\leq\; \exp\left(\frac{y(1-x)}{1+x\frac{y}{Q}}\right) \leq\; \exp(y(1-x)) \qquad (55)$$

We have that $\text{OPT}_1(a,s)$is decreasing in s for constant $a<1$. (56)

Let $a=\frac{1}{2},\; c \;=\; \frac{2}{Q}$.

We have by (55) FIRSUM$(a,c,s) \;<\; \exp(1)$

SECSUM(a,c,s) is decreasing in $s\geq 0$.

(As can be shown by elementary means.)

$\text{OPT}_1(a,s)\,(\text{SECSUM}(a,c,s)+\exp(1)) \;<\; 3.913$ for $s=5$

and decreasing in s with (56)

Let $a=\frac{2}{3},\; c \;=\; \frac{2}{Q}$.

We have FIRSUM$(a,c,s) \;<\; \exp(2/3)$

SECSUM(a,c,s) is decreasing in $s\geq 0$.

$\text{OPT}_1(a,s)\,(\text{SECSUM}(a,c,s)+\exp(2/3)) \;<\; 3.962$ for $s=4$

and decreasing in s with (56)

Let $a=\frac{2}{3},\; c \;=\; \frac{3}{Q}$. We have FIRSUM$(a,c,s) \;<\; \exp(1)$

SECSUM(a,c,s) is decreasing in $s\geq 2$.

$\text{OPT}_1(a,s)\,(\text{SECSUM}(a,c,s)+\exp(1)) \;<\; 3.985$ for $s=6$

and decreasing in s with (56)

Let $a = 1 - 7/(15Q),\ c = 3/Q$.
$\mathrm{OPT}_1(a, s)$ is increasing in s to $3\exp(-7/15) + 1$.
FIRSUM $(a, c, s),$ SECSUM$(a, c, s)$are both decreasing in s.
$(3\exp(-7/15) + 1)\,(\mathrm{SECSUM}(a, c, s) + \mathrm{FIRSUM}(a, c, s))\ <\ 3.9$ for $s = 4$

The case $a = 1\ -\ \frac{7}{15Q}$ and $c = 1$ is included in Lemma 33.

3 Proof of Theorem 28 for $d = 4,\ \lambda \geq 1 - 1/d, s \geq 5.$

We fix $a = 1$. Observe that $B(1/c)$ in the subsequent lemma goes from 1 to $1 - 1/(2Q)$ for $c \geq 3$.

Lemma 37 *Let* $B(x) = B(x, s) = 1 + 3/(2Q)x - 1/(2Q)$. *Then OPT*$(1, B(1/c), c, s)$ *is strictly decreasing in* $c \geq 3$.

Proof of Theorem 28 for $\lambda \geq 1 - 1/d$. We have $\lambda/(1 - \lambda) \geq d - 1$. For each $P \geq d - 1$ we have c such that $P = \frac{c}{B(1/c)}$. As $\mathrm{OPT}(1, 1, 3, s) = 4$ the Theorem follows. □

Proof of Lemma 37. We rewrite $\mathrm{OPT}(1, B(1/c), c, s)$ first. We multiply OPT_2 with c^Q and OPT_3 with $1/c^Q$ and get (using $c \geq 3$ to get rid of the absolute value) $\mathrm{OPT}(1, B(1/c, s), c, s)\ =$

$$= \left(3 + \frac{q(B(1/c, s)s)}{q(s)}\right)\left(\frac{1}{\frac{B(1/c,s)}{c} + 1}\right)^Q \left(\left(\frac{1}{c} + 1\right)^Q + 3\left(\frac{1}{3} - \frac{1}{c}\right)^Q\right).$$

We substitute c for $1/c$ in the preceding equation. The claim follows from

$$\left(3 + \frac{q(B(c))s)}{q(s)}\right)\left(\frac{1}{B(c)c + 1}\right)^Q \left((c + 1)^Q + 3\left(\frac{1}{3} - c\right)^Q\right)$$

increases in $0\ <\ c\ <\ 1/3.$ (57)

We use the following notation in the sequel:

$$\mathrm{OPT}_1(b,s) = 3 + \frac{q(sb)}{q(s)}\,,\ \mathrm{OPT}_2(b,c,s)\ =\ \left(\frac{1}{bc+1}\right)^Q,$$

$$\mathrm{OPT}_3(c,s) = (c+1)^Q +\ 3\left(\frac{1}{3}-c\right)^Q,\ c \le \frac{1}{3}$$

$$\mathrm{OPT}(b,c,s) = \mathrm{OPT}_1(b,s)\mathrm{OPT}_2(b,c,s)\mathrm{OPT}_3(c,s).$$

For $b=1, c=\dfrac{1}{3}$ we have $\mathrm{OPT}(b,c,s)=4$. We abbreviate

$$\text{PM}(x,y) = (x+1)^y - 3\left(\frac{1}{3}-x\right)^y,\ x \le \frac{1}{3}$$

$$\text{PP}(x,y) = (x+1)^y + 3\left(\frac{1}{3}-x\right)^y,\ x \le \frac{1}{3}$$

$$B\ = B(c,s),\quad B' = \frac{\partial}{\partial c}B = \frac{3}{2Q},\quad q'(x) = \exp(x)-1$$

$$q(x) = \exp(x)-x-1,\quad \frac{\partial}{\partial c}\ln(\mathrm{OPT}(B,c,s) >=< 0$$

$$\Longleftrightarrow \frac{\frac{B'sq'(sB)}{q(s)}}{3+\frac{q(sB)}{q(s)}} - Q\frac{B'c+B}{1+Bc} + Q\frac{\text{PM}(c,Q-1)}{\text{PP}(c,Q)} > 0$$

$$\Longleftrightarrow \frac{\frac{B'q'(sB)}{q'(s)}}{3+\frac{q(sB)}{q(s)}} - \frac{B'c+B}{1+Bc} + \frac{\text{PM}(c,Q-1)}{\text{PP}(c,Q)} >=< 0.(\text{ Division by } Q.) \tag{58}$$

For $c=\frac{1}{3}$ we have $\mathrm{OPT}(B,1/3,s)=4$, and the derivative is 0. We split (58) into two additive terms. The following two inequalities directly imply (57.)

$$\frac{\frac{B'q'(sB)}{q'(s)}}{3+\frac{q(sB)}{q(s)}} - \frac{B'c}{1+Bc} > 0 \tag{59}$$

$$\frac{\text{PM}(c,Q-1)}{\text{PP}(c,Q)} - \frac{B}{1+Bc} > 0 \tag{60}$$

Proof of (59) for $s>2$. Let $K=\frac{q'(sB)}{q'(s)}$ and $L=\frac{q(sB)}{q(s)}$. By (7) we have $L \le K$, and as $B'>0$ it is sufficient to show

$$\frac{K}{3+K} > \frac{c}{1+Bc} \Leftrightarrow K(1+Bc-c) > 3c.$$

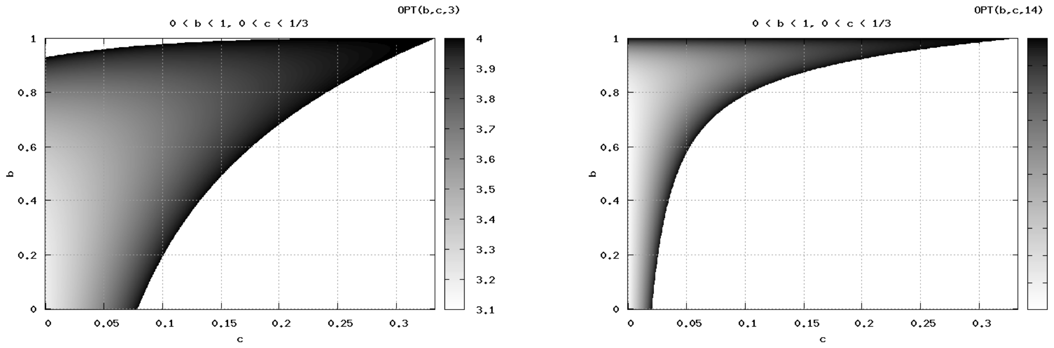


Fig. 3. OPT(b, c, s) over the rectangle $0 \leq b \leq 1, 0 \leq c \leq 1/3$ for $s = 3$ and $s = 14$.

For $c = \frac{1}{3}$ both sides of the preceding inequality are $= 1$. It is easy to observe that $K(1 + Bc - c)$ is convex in c for $c > 1/(3 \cdot 2)$. (Cf. proof of Lemma 20) and $3c$ is a linear function. If at $c = \frac{1}{3}$ the derivative of $3c$ is greater than the derivate of $K(1 + Bc - c)$ the second intersection of both sides (if any) lies at some point $c > \frac{1}{3}$ and the claim holds for $1/(3 \cdot 2 < c < \frac{1}{3}$. For $c < 1/(3 \cdot 2)$ we argue as in the proofs of the Lemmas mentioned above. Therefore it is sufficient to show that at $c = \frac{1}{3}$

$$\frac{\partial}{\partial c} K(1 + Bc - c) < \frac{\partial}{\partial c} 3c.$$

We have

$$K' = \frac{B' s \exp(sB)}{\exp(s) - 1}.$$

and at $c = 1/3$

$$K'(\underbrace{1 + Bc - c}_{=1}) + \underbrace{K}_{=1}(\underbrace{B'c + B - 1}_{=1/2Q}) < 3$$

$$\Leftrightarrow \frac{3(\exp(s) - s - 1)\exp(s)}{2(\exp(s) - 1)^2} + \frac{\exp(s) - s - 1}{2s(\exp(s - 1)} < 3 \qquad (61)$$

We omit the proof that inequality (61) holds for $s \geq 2$.

Proof of (60) for $s \geq 5$. As in (49) inequality (60) is equivalent to

$$B < \frac{\text{PM}(c, Q - 1)}{\text{PP}(c, Q - 1} \qquad (62)$$

The left hand side is a linear function in c and the right hand side a strictly increasing, concave function in c. For $c = \frac{1}{3}$ both sides of (62) are 1. So we must show that (62) holds for $c = 0$. Setting $c = 0$ leads to

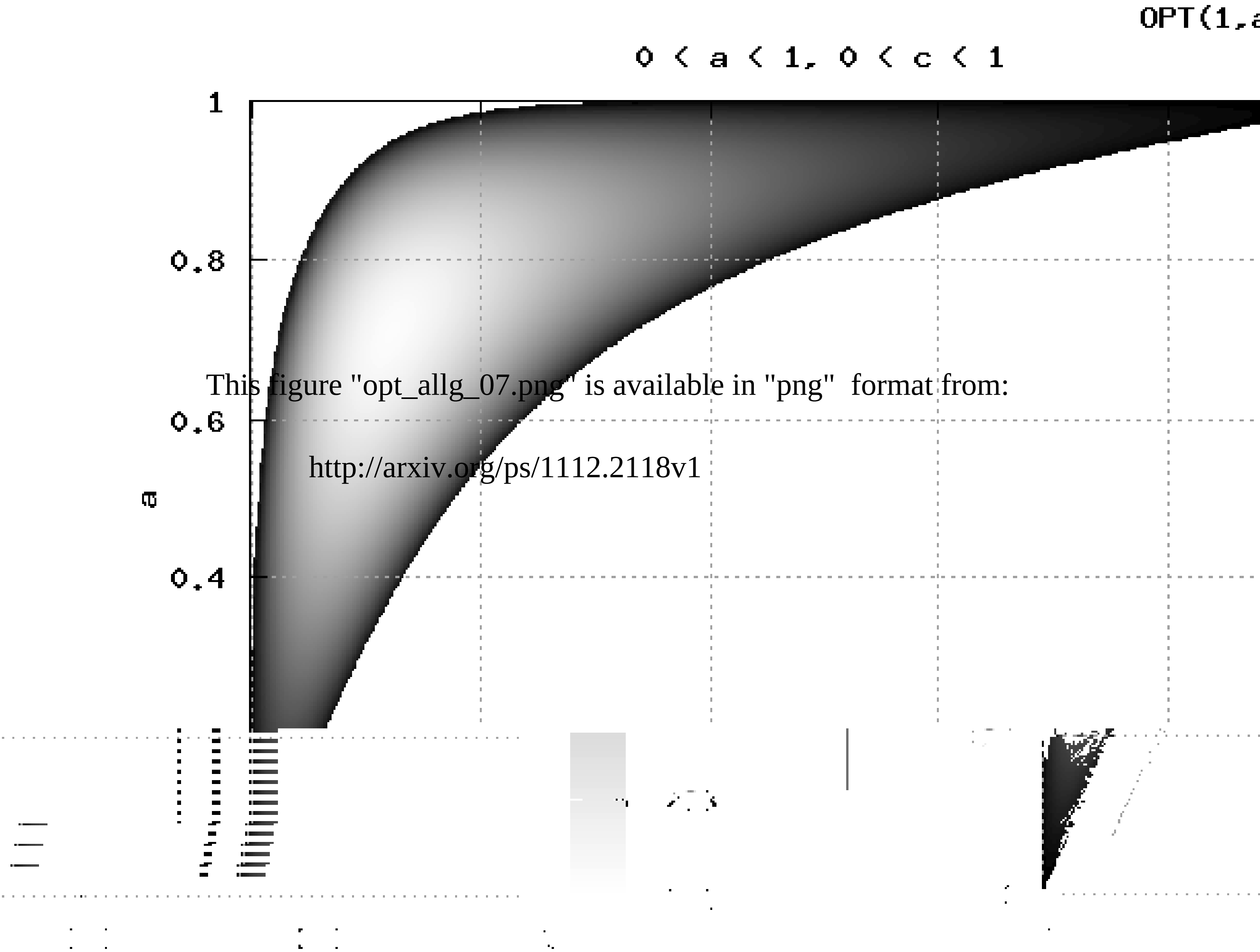
$$1 - \frac{1}{2Q} < \frac{1 - 3\left(\frac{1}{3}\right)^{Q-1}}{1 + 3\left(\frac{1}{3}\right)^{Q-1}} = \frac{1 - \left(\frac{1}{3}\right)^{Q-2}}{1 + \left(\frac{1}{3}\right)^{Q-2}}.$$

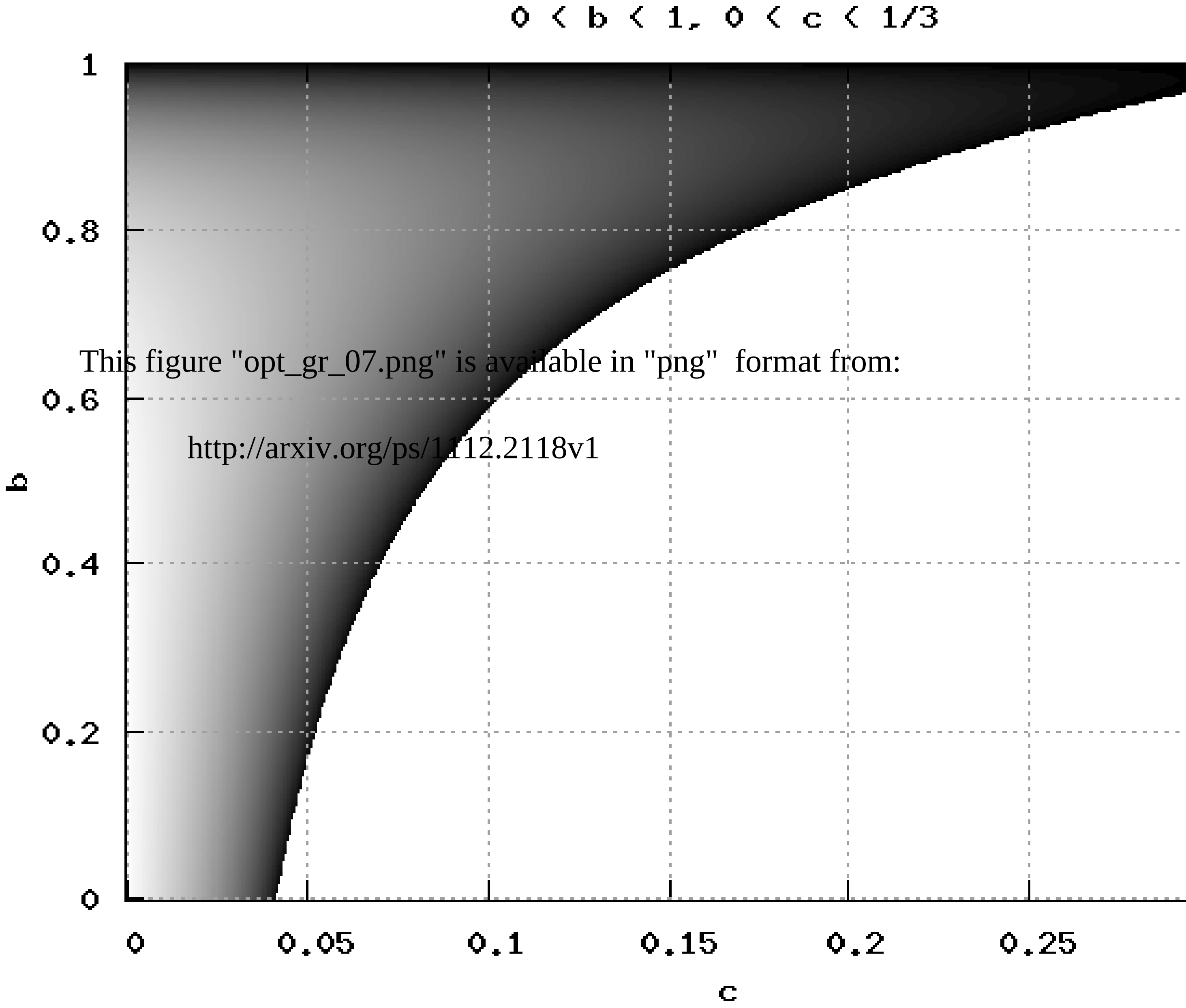
For $Q = 5$ we get $\frac{9}{10} < \frac{13}{14}$. We omit the argument that the last inequality holds for all $Q \geq 5$ and therefore as $Q > s$ for all $s \geq 5$.

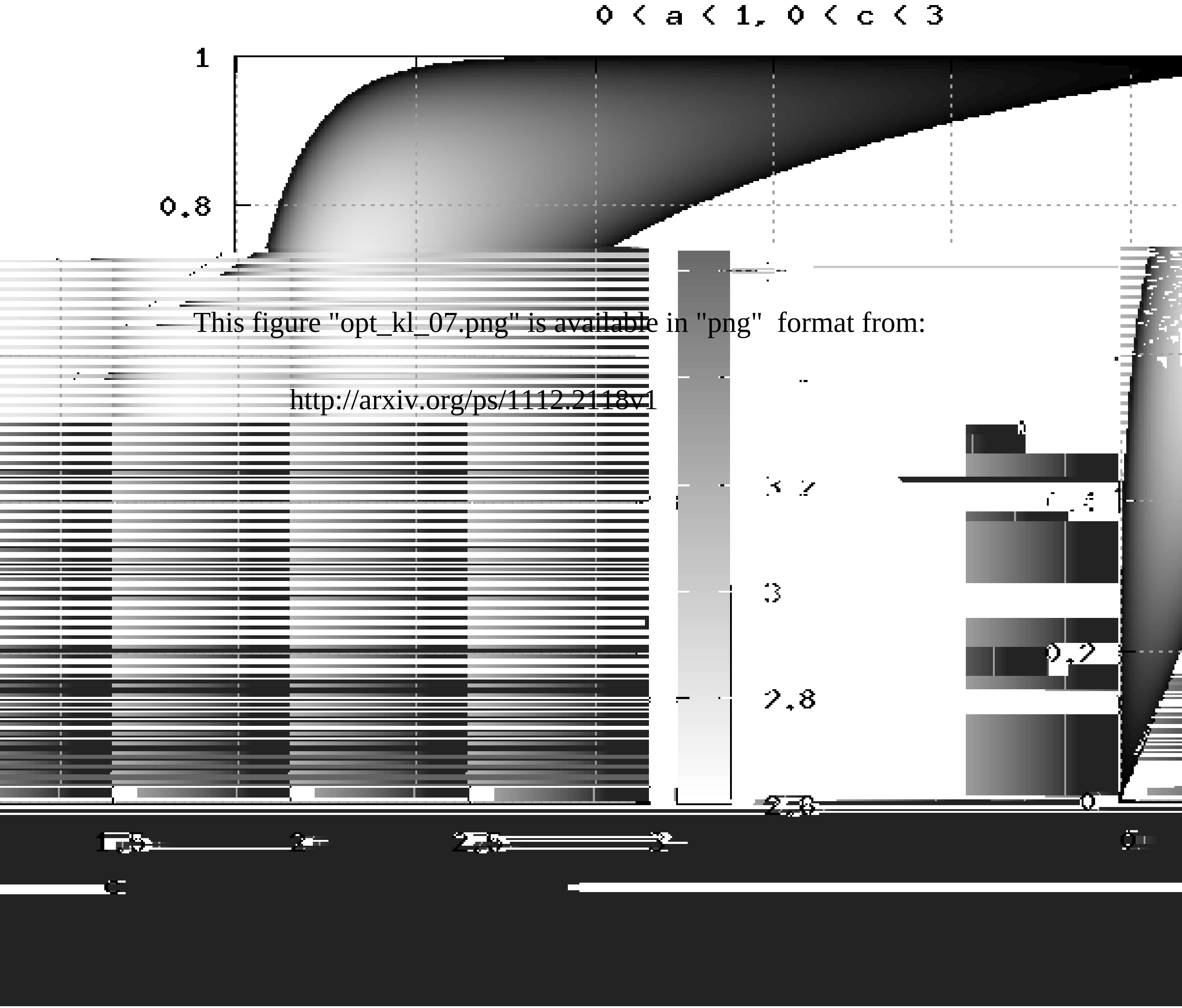
References

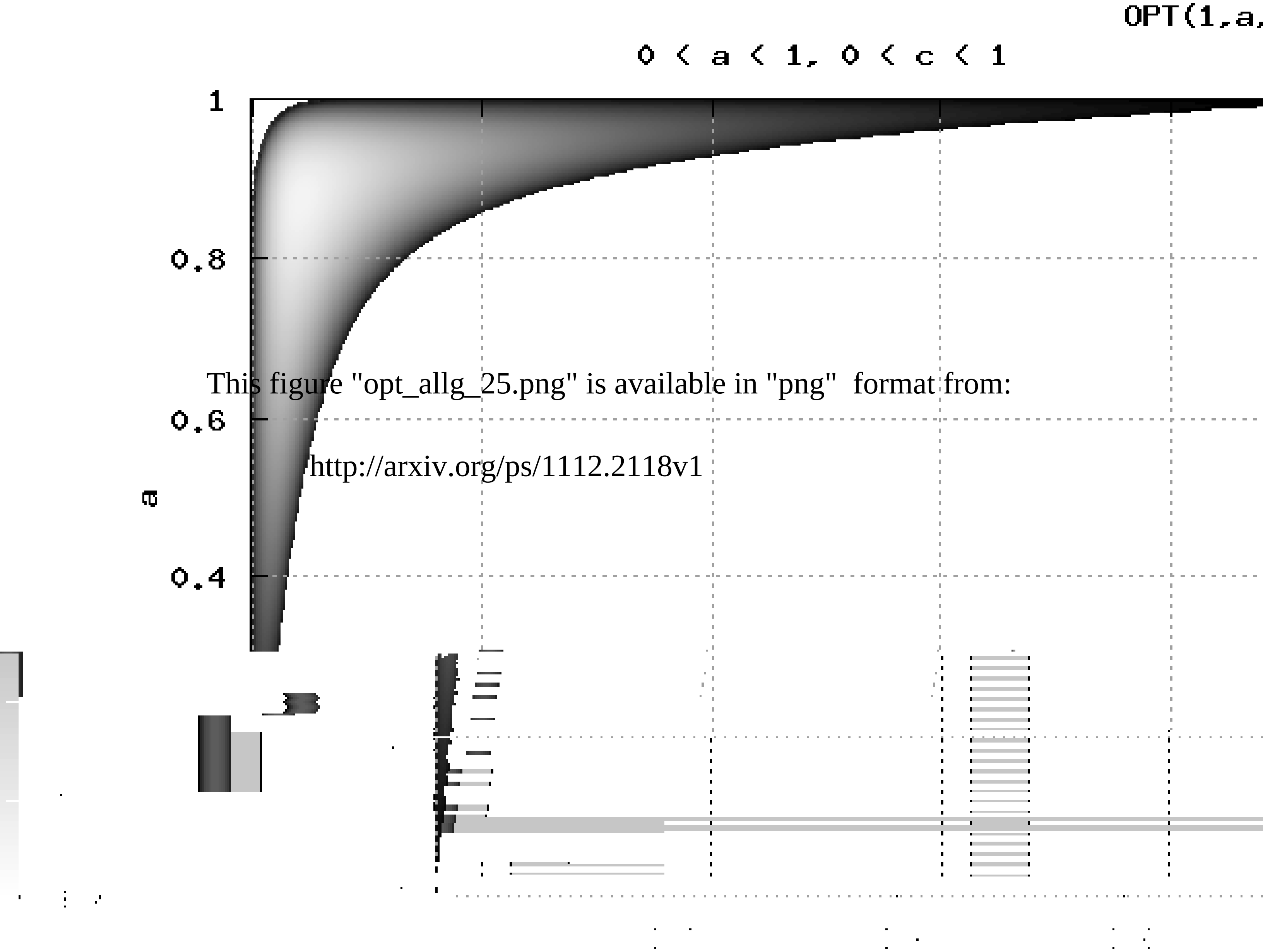
1. J. Diaz et al. On the satisfiability threshold of formulas with three literals per clause. Theoretical Computer Science 410 (2009) 2920 - 2934.
2. M Molloy. Cores in random hypergraphs and boolean formulas. Random Stuctures and Algorithms 27, 2005, 124 - 135.
3. J. Hastad. Some optimal inapproximability results. J. ACM 48, 2001, 798 – 859.
4. R. Durrett. Probability Theory: Theory and Examples. Wadsworth and Brooks 1991.
5. M Dietzfelbinger et al. Tight thresholds for Cuckoo Hashing via XORSAT. CoRR, 2009, abs/0912.0287. See also Proceedings ICALP 2010, LNCS 6198, 213 - 225.
6. H. Connamacher, M. Molloy. The exact satisfiability threshold for a potentially in tractable random constraint satisfaction problem. Proceedings 45th FoCS 2004, 590 - 599.
7. Michael Molloy. Models for Random Constraint Satisfaction Problems. SIAM J. Comput. 32(4), 2003, 935-949.
8. O. Dubois, J. Mandler. The $3-$XORSAT satisfiability threshold. Proceedings 43rd FoCS 2003, 769.
9. N. Creignou, H. Daudé. The SAT-UNSAT transition for random constraint satisfaction problems. Discrete Mathematics 309 (8), 2085 - 2099.
10. V. F. Kolchin. Random graphs and systems of linear equations in finite fields. Random Structures and Algorithms 5, 1995, 425 - 436.
11. A. Braunstein, M. Mezard, R. Zecchina. Survey propagation: an algorithm for satisfiability. arXiv:cs/0212002.
12. Amin Coja-Oghlan, Angelica Y. Pachon-Pinzon. The Decimation Process in Random k-SAT. In Proceedings ICALP (1) 2011, 305-316.
13. Ehud Friedgut. Hunting for sharp thresholds. Random Struct. Algorithms 26(1-2), 2005, 37-51.
14. Andreas Goerdt. On Random Betweenness Constraints. Combinatorics, Probability and Computing 19(5-6), 2010, 775-790
15. D. Achlioptas, C. Moore. Random k-SAT: Two Moments Suffice to Cross a Sharp Threshold. SIAM J. Comput. 36(3), 2006, 740-762
16. V. Puyhaubert. Generating functions and the satisfiability threshold. Discrete Mathematics and Theoretical Computer Science 6, 2004, 425, - 436.
17. H. Connamacher. Exact thresholds for DPLL on random XOR-SAT and NP-complete extensions of XOR-SAT. Theoretical Computer Science 2011.
18. A. Meisels, S. E. Shimony, G. Solotorevsky. Bayes Networks for estimating the number of solutions to a CSP. Proceedings AAAI 1997, 179 - 184.
19. M. Luby, M. Mitzenmacher, A. Shokrollahi, D. A. Spielman. Efficient erasure coeds. IEEE Trans. Inform. Theory 47(2), 2001, 569 - 584.
20. T. J. Richardson, R. Urbanke. Modern Coding Theory. Cambridge University Press, 2008.
21. Dimitris Achlioptas, Morteza Ibrahimi, Yashodhan Kanoria, Matt Kraning, Mike Molloy and Andrea Montanari. The Set of Solutions of Random XORSAT Formulae. In Proceedings SoDA 2012.

22. N. G. de Bruijn. Asymptotic Methods in Analysis. North Holland 1958,
23. N. Bhattacharya, R. Ranga Rao. Normal Approximation and Asymptotic Expansions. Robert E. Krieger Publishing Company, 1986.
24. M. Mitzenmacher, Eli Upfal. Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press 2005.


OPT(1,a
0 < a < 1, 0 < c < 1
1
0.8
0.6
0.4
a

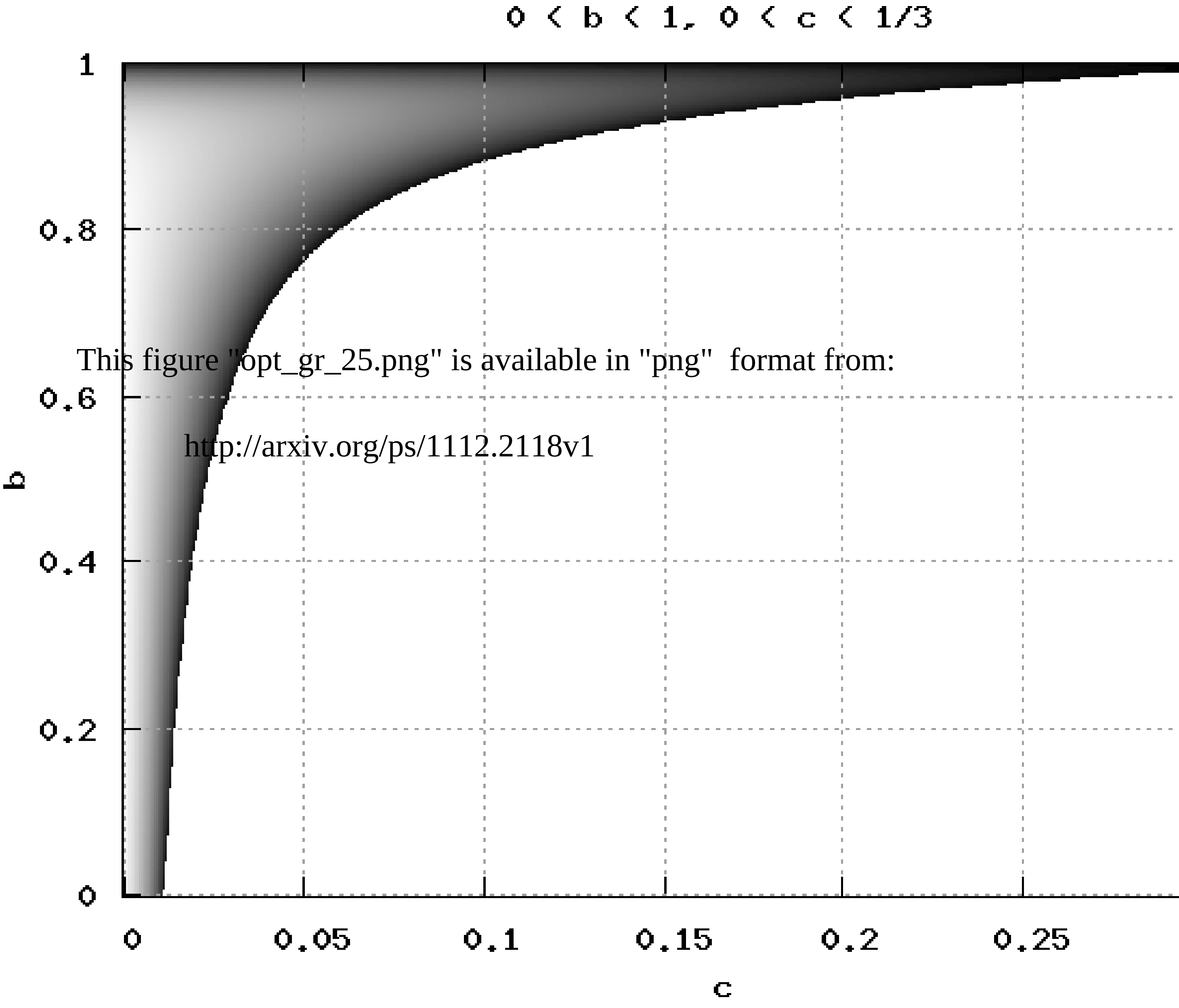

0 < b < 1, 0 < c < 1/3
1
0.8
0.6
0.4
0.2
0
b
0
0.05
0.1
0.15
0.2
0.25
c

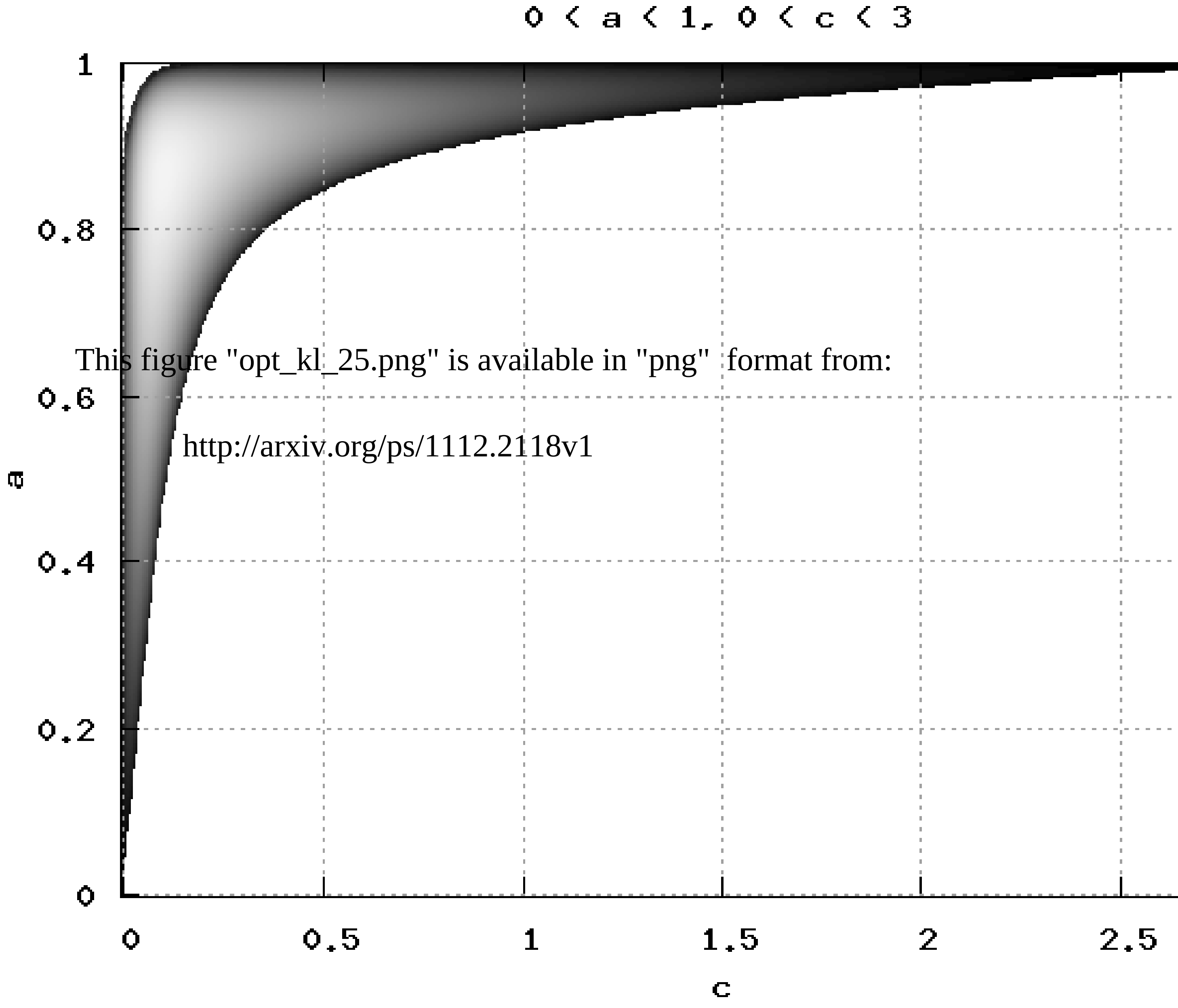

0 < a < 1, 0 < c < 3
1
0.8
3.2
3
2.8
0.4
0.2
0
2
3
c



This figure "opt_allg_25.png" is available in "png" format from:

http://arxiv.org/ps/1112.2118v1


0 < b < 1, 0 < c < 1/3
1
0.8
0.6
0.4
0.2
0
b
0
0.05
0.1
0.15
0.2
0.25
c


0 < a < 1, 0 < c < 3
1
0.8
0.6
0.4
0.2
0
a
0
0.5
1
1.5
2
2.5
c